kaspersky

Kaspersky Security Center 16.3 Linux

© 2026 AO Kaspersky Lab

Inhalt

Hilfe zu Kaspersky Security Center Linux

Neuerungen

Behobene Probleme

Über Kaspersky Security Center Linux

- Lieferumfang
- Hard- und Softwarevoraussetzungen
  - Anforderungen an den Administrationsserver
  - Anforderungen an die Web Console
  - Anforderungen an den Administrationsagenten
- Kompatible Anwendungen und Lösungen von Kaspersky
- Über die Kompatibilität der Kaspersky Security Center Linux-Komponenten
- Vergleich von Kaspersky Security Center: Windows-basiert vs. Linux-basiert
- Über die Kaspersky Security Center Cloud Console

Architektur und grundlegende Konzepte

- Architektur
- Bereitstellungsdiagramm für Kaspersky Security Center Linux Administrationsserver und Kaspersky Security Center Web Console
- Ports, die von Kaspersky Security Center Linux verwendet werden
- Von Kaspersky Security Center Web Console verwendete Ports
- Grundbegriffe
  - Administrationsserver
  - Hierarchie des Administrationsservers
  - Virtueller Administrationsserver
  - Webserver
  - Kaspersky Security Center Linux Webserver
  - Administrationsagent
  - Administrationsgruppen
  - Verwaltetes Gerät
  - Nicht zugeordnetes Gerät
  - Administrator-Arbeitsplatz
  - Web-Plug-ins zur Verwaltung
  - Richtlinien
  - Richtlinienprofile
  - Aufgaben
  - Aufgabenumfang
  - Interaktion von Richtlinien und lokalen Programmeinstellungen
  - Verteilungspunkt
  - Verbindungs-Gateway
  - Virtuelle Administrationsserver

Schemata für Datenverkehr und Portnutzung

- Administrationsserver und verwaltete Geräte im LAN
- Primärer Administrationsserver im LAN und zwei sekundäre Administrationsserver
- Administrationsserver im LAN, verwaltete Geräte im Internet und Verwendung eines Reverse-Proxys

Administrationsserver im LAN, verwaltete Geräte im Internet; Verwendung eines Verbindungs-Gateways
Administrationsserver in der DMZ, verwaltete Geräte im Internet
Interaktion der Komponenten von Kaspersky Security Center Linux und der Sicherheitsanwendungen: weitere Informationen
Konventionen für die Interaktionsschemata
Administrationsserver und DBMS
Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendung
Software-Upgrades auf dem Client-Gerät mithilfe des Verteilungspunkts
Hierarchie der Administrationsserver: primärer Administrationsserver und sekundärer Administrationsserver
Hierarchie der Administrationsserver mit sekundärem Administrationsserver in der demilitarisierten Zone
Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät
Administrationsserver und zwei Geräte in der DMZ: ein Verbindungs-Gateway und ein Client-Gerät
Administrationsserver und Kaspersky Security Center Web Console
Erste Schritte
Härtungsleitfaden
Checkliste zur Härtung
Bereitstellung des Administrationsservers
Verbindungssicherheit
Konten und Authentifizierung
Verwaltung des Schutzes des Administrationsservers
Verwaltung des Schutzes der Client-Geräte
Konfigurieren des Schutzes für verwaltete Programme
Wartung des Administrationsservers
Ereignisübertragung an Systeme von Dritten
Sicherheitsempfehlungen für Drittanbieter-Informationssysteme
Empfehlungen für die Verwendung von Kaspersky-Sicherheitsanwendungen
Szenario: Authentifizierung am MySQL-Server
Szenario: Authentifizierung am PostgreSQL-Server
Vorbereitung der Bereitstellung
Konfiguration von Kaspersky Security Center Linux auswählen
Typische Konfiguration: Einzelbüro
Typische Konfiguration: Mehrere größere Büros mit eigenen Administratoren
Typische Konfiguration: Mehrere kleine Remote-Büros
Struktur des Schutzes im Unternehmen auswählen
Typische Vorgehensweisen der Bereitstellung
Auswahl des DBMS
Internetzugriff für den Administrationsserver bereitstellen
Internetzugriff: Administrationsserver in einem lokalen Netzwerk
Zugriff aus dem Internet: Administrationsserver in der demilitarisierten Zone
Installation
Den MariaDB x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren
PostgreSQL- oder Postgres Pro-Server für die Ausführung mit Kaspersky Security Center Linux konfigurieren
Den MySQL x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren
Ein hochverfügbares DBMS-Cluster für die Arbeit mit Kaspersky Security Center Linux vorbereiten
Kaspersky Security Center Linux installieren
Kaspersky Security Center Linux im Silent-Modus installieren
Kaspersky Security Center Linux unter Astra Linux in der geschlossenen Softwareumgebung installieren

Kaspersky Security Center Web Console installieren
Installationsparameter für Kaspersky Security Center Web Console
Kaspersky Security Center Web Console unter Astra Linux in der geschlossenen Softwareumgebung installieren
Kaspersky Security Center Linux mittels Skript installieren
Kaspersky Security Center Linux Failover-Cluster bereitstellen
Kaspersky Security Center Linux Failover-Cluster. Bereitstellungsschemata
Kaspersky Security Center Linux Failover-Cluster
Szenario: Kaspersky Security Center Linux Failover-Cluster bereitstellen
Kaspersky Security Center Linux Failover-Cluster. Hard- und Softwarevoraussetzungen
Einen Dateiserver für ein Kaspersky Security Center Linux Failover-Cluster vorbereiten
Knoten für ein Kaspersky Security Center Linux Failover-Cluster vorbereiten
Kaspersky Security Center Linux auf den Knoten des Kaspersky Security Center Linux Failover-Clusters installieren
Cluster-Knoten manuell starten und beenden
Knoten eines Failover-Clusters neu installieren
Kaspersky Security Center Web Console mit Verbindung zum Administrationsserver installieren, welcher auf Knoten des Kaspersky Security Center Linux Failover-Clusters bereitgestellt wurde
Geografisch verteiltes Kaspersky Security Center Linux Failover-Cluster
Geografisch verteiltes Cluster mit Ubuntu und PostgreSQL-DBMS
Dateisystem der Cluster-Knoten vorbereiten
Eines repliziertes Cluster-Dateisystem vorbereiten
Corosync und Pacemaker auf den Cluster-Knoten installieren und konfigurieren
PostgreSQL-DBMS installieren und konfigurieren
Kaspersky Security Center Linux auf den Knoten eines geografisch verteilten Failover-Clusters installieren
Geografisch verteiltes Cluster mit SberLinux und Platform V Pangolin-DBMS
Dateisystem der Cluster-Knoten vorbereiten
Eines repliziertes Cluster-Dateisystem vorbereiten
Corosync und Pacemaker auf den Cluster-Knoten installieren und konfigurieren
Installation und Konfiguration des DBMS Platform V Pangolin
Kaspersky Security Center Linux auf den Knoten eines geografisch verteilten Failover-Clusters installieren
Kaspersky Security Center Web Console auf den Knoten eines geografisch verteilten Failover-Clusters installieren
Benutzerkonten für die Arbeit mit DBMS
DBMS-Benutzerkonto für die Arbeit mit MySQL und MariaDB konfigurieren
DBMS-Benutzerkonto für die Arbeit mit PostgreSQL und Postgres Pro konfigurieren
In MySQL und MariaDB-DBMS Daten aus einem freigegebenen Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich verschieben
Zertifikate für die Ausführung mit Kaspersky Security Center Linux
Über die Zertifikate von Kaspersky Security Center
Anforderungen an benutzerdefinierte Zertifikate für deren Verwendung in Kaspersky Security Center Linux
Zertifikat für Kaspersky Security Center Web Console neu ausstellen
Zertifikat für Kaspersky Security Center Web Console ersetzen
Konvertieren eines pfx-Zertifikats in ein pem-Zertifikat
Szenario: Angeben des benutzerdefinierten Zertifikats des Administrationsservers
Zertifikats des Administrationsservers mittels Dienstprogramm klsetsrvcert ersetzen
Administrationsagenten mit dem Administrationsserver mittels Dienstprogramm klmover verbinden
Webserver-Zertifikat neu ausstellen
Das standardmäßige IAM-Zertifikats in ein benutzerdefiniertes Zertifikat ändern
Adresse des Administrationsservers zur Konfiguration des IAM-Servers hinzufügen

Den freigegebenen Ordner angeben
In der Kaspersky Security Center Web Console anmelden und abmelden
Benutzeroberfläche der Kaspersky Security Center Web Console
Sprache der Benutzeroberfläche von Kaspersky Security Center Web Console ändern
Startseite der Kaspersky Security Center Web Console anpassen
Lesezeichen hinzufügen und entfernen
Kaspersky Security Center Web Console entfernen
Schnellstartassistent
Schritt 1. Einstellungen für die Internetverbindung festlegen
Schritt 2. Erforderliche Updates herunterladen
Schritt 3. Zu sichernde Assets auswählen
Schritt 4. Verwendete Verschlüsselung für die Lösungen auswählen
Schritt 5. Plug-ins für verwaltete Programme konfigurieren
Schritt 6. Programmpakete herunterladen und Installationspakete erstellen
Schritt 7. Kaspersky Security Network konfigurieren
Schritt 8. Methode zur Programmaktivierung auswählen
Schritt 9. Einstellungen zur Verwaltung von Drittanbieter-Updates festlegen
Schritt 10. Erstellen einer grundlegenden Konfiguration für Netzwerkschutz
Schritt 11. E-Mail-Benachrichtigungen konfigurieren
Schritt 12. Schnellstartassistent abschließen
Assistent für die Bereitstellung des Schutzes
Schritt 1. Assistent für die Bereitstellung des Schutzes starten
Schritt 2. Installationspaket auswählen
Schritt 3. Verteilungsmethode der Schlüsseldatei oder des Aktivierungscodes auswählen
Schritt 4. Auswählen der Version des Administrationsagenten
Schritt 5. Auswählen der Geräte
Schritt 6. Festlegen der Einstellungen für die Aufgabe zur Remote-Installation
Schritt 7. Verwaltung des Neustarts
Schritt 8. Deinstallieren inkompatibler Programme vor der Installation
Schritt 9. Verschieben von Geräten in die Gruppe "Verwaltete Geräte"
Schritt 10. Auswählen von Benutzerkonten für den Zugriff auf Geräten
Schritt 11. Beginnen der Installation
Kaspersky Security Center Linux aktualisieren
Kaspersky Security Center Linux ab Version 16 aktualisieren
Kaspersky Security Center Linux ab Version 16 mittels Installationsdatei aktualisieren
Kaspersky Security Center Linux ab Version 16 mittels Backup aktualisieren
Kaspersky Security Center Linux ab Version 16 auf den Knoten des Kaspersky Security Center Linux Failover-Clusters aktualisieren
Kaspersky Security Center Linux ab Version 15.4 oder früher aktualisieren
Kaspersky Security Center Linux Version 15.4 oder früher mittels Installationsdatei aktualisieren
Kaspersky Security Center Linux Version 15.4 oder früher mittels Backup aktualisieren
Kaspersky Security Center Linux Version 15.4 oder früher auf den Knoten des Kaspersky Security Center Linux Failover-Clusters aktualisieren
Kaspersky Security Center Web Console aktualisieren
Kaspersky Security Center Web Console unter Astra Linux in der geschlossenen Softwareumgebung aktualisieren

Migration nach Kaspersky Security Center Linux
Migration auf Kaspersky Security Center Linux mittels Daten-Backup des Administrationsservers
Video: Migration auf Kaspersky Security Center Linux mittels Daten-Backup des Administrationsservers
Migration zu Kaspersky Security Center Linux mittels Migrationsassistenten
Gruppenobjekte aus Kaspersky Security Center Windows exportieren
Importieren der Exportdatei in Kaspersky Security Center Linux
Verwaltete Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen
Administrationsserver konfigurieren
Verbindungsadresse des Administrationsservers konfigurieren
Verbindung zwischen Kaspersky Security Center Web Console und Administrationsserver anpassen
Allow-Liste mit IP-Adressen für die Verbindung mit Kaspersky Security Center Linux konfigurieren
Die Internetzugriffseinstellungen für den Administrationsserver konfigurieren
Hierarchie des Administrationsservers
Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen
Liste mit sekundären Administrationsservern anzeigen
Virtuelle Administrationsserver verwalten
Einen virtuellen Administrationsserver erstellen
Einen virtuellen Administrationsserver aktivieren und deaktivieren
Einem virtuellen Administrationsserver einen Administrator zuweisen
Den Administrationsserver für Client-Geräte ändern
Einen virtuellen Administrationsserver löschen
Protokollierung der Verbindungsereignisse des Administrationsservers konfigurieren
Maximalen Anzahl an Ereignissen in der Ereignis-Datenverwaltung festlegen
Administrationsserver auf anderes Gerät übertragen
DBMS-Anmeldedaten ändern
Daten des Administrationsservers sichern und wiederherstellen
Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers erstellen
Tool "klbackup" zum Sichern und Wiederherstellen von Daten verwenden
Das klbackup-Tool verwenden, um verwaltete Geräte unter die Verwaltung eines anderen Administrationsservers zu stellen
Daten des Administrationsservers bei Verwendung von MySQL oder MariaDB sichern und wiederherstellen
Wartung des Administrationsservers
Administrationsserver-Hierarchie löschen
Zugriff auf öffentliche DNS-Server
Schnittstelle konfigurieren
Geschützte Verbindung mit dem Administrationsserver einrichten
Kommunikation mit TLS verschlüsseln
Netzwerkeinstellungen zur Interaktion mit externen Diensten
Globale Liste der Subnetze
Integrität der Module anhand der Tools klscmodchk und integrity_checker prüfen
Geräte im Netzwerk finden
Szenario: Netzwerkgeräte finden
Windows-Netzwerkabfrage
IP-Bereiche abfragen
IP-Bereich hinzufügen und bearbeiten
Zeroconf-Abfrage
Abfrage des Domänencontrollers
Authentifizierung und Verbindung mit einem Domänencontroller

Einen Samba-Domänencontroller konfigurieren
Arbeitsgerätebestand
Informationen über neue Geräte hinzufügen
Kriterien zur Erkennung von Unternehmensgeräten anpassen
Dynamischen VDI-Modus auf Client-Geräten verwenden
Dynamischen VDI-Modus in den Eigenschaften des Installationspakets des Administrationsagenten aktivieren
Geräte, die zu VDI gehören, in eine Administrationsgruppe verschieben
Client-Geräte verwalten
Einstellungen eines verwalteten Geräts
Verbindung des Client-Geräts mit dem Administrationsserver manuell prüfen. Tool klnagchk
Verschiebungsregeln für Geräte
Regeln für das Verschieben von Geräten erstellen
Regeln für das Verschieben von Geräten kopieren
Bedingungen für Verschiebungsregeln für Geräte
Geräte manuell zu einer Administrationsgruppe hinzufügen
Manuelles Verschieben von Geräten oder Clustern in eine Administrationsgruppe
Über Cluster und Server-Arrays
Eigenschaften eines Cluster- oder Server-Arrays
Verteilungspunkte und Verbindungs-Gateways anpassen
Über Verteilungspunkte
Typische Konfiguration von Verteilungspunkten: Einzelbüro
Typische Konfiguration von Verteilungspunkten: Mehrere kleine, eigenständige Büros
Anzahl und Konfiguration der Verteilungspunkte bestimmen
Verteilungspunkte automatisch zuweisen
Verteilungspunkte manuell zuweisen
Hinzufügen eines Verbindungs-Gateways als Verteilungspunkt innerhalb der DMZ
Liste mit Verteilungspunkten für eine Administrationsgruppe bearbeiten
Push-Server aktivieren
Anzahl der Datei-Deskriptoren für den klnagent-Dienst erhöhen
Über die Varianten für den Gerätestatus
Wechsel der Statuswerte von Geräten konfigurieren
Geräteauswahlen
Geräteliste einer Geräteauswahl anzeigen
Geräteauswahl erstellen
Einstellungen einer Geräteauswahl anpassen
Geräteliste einer Geräteauswahl exportieren
Geräte in der Auswahl aus Administrationsgruppen löschen
Geräte-Tags
Geräte-Tag erstellen
Geräte-Tag umbenennen
Geräte-Tag löschen
Geräte mit zugewiesenen Tags anzeigen
Tags anzeigen, die einem Gerät zugewiesen sind
Tags einem Gerät manuell zuweisen
Zugewiesene Tags von einem Gerät entfernen
Regeln für das automatische Zuweisen von Tags an Geräten anzeigen
Regeln für das automatische Zuweisen von Tags an Geräte bearbeiten

Regeln für das automatische Zuweisen von Tags an Geräte erstellen

Regeln für das automatische Zuweisen von Tags an Geräte ausführen

Regeln für das automatische Zuweisen von Tags an Geräte löschen

Verwalten von Geräte-Tags mit dem Tool klscflag

Verschlüsselung und Datenschutz

Liste der verschlüsselten Laufwerke anzeigen

Liste der Verschlüsselungsereignisse anzeigen

Verschlüsselungsberichte erstellen und anzeigen

Zugriff auf ein verschlüsseltes Laufwerk im autonomen Modus gewähren

Übertragung von Chiffrierschlüsseln zwischen Administrationsservern

Den Administrationsserver für Client-Geräte ändern

Konflikte zwischen mehreren Administrationsservern vermeiden

Geräte, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind, auf einen anderen Administrationsserver verschieben

Maßnahmen anzeigen und konfigurieren, wenn Geräte als inaktiv angezeigt werden

Nachricht an Gerätenutzer senden

Client-Geräte von einem entfernten Standort einschalten, ausschalten und Neustart durchführen

Remote-Zugriff auf verwaltete Geräte

Remote-Zugriff von einem Linux-basierten Gerät mit Kaspersky Security Center Web Console auf ein verwaltetes Linux-Gerät

Remote-Zugriff von einem Linux-basierten Gerät mit Kaspersky Security Center Web Console auf ein verwaltetes Windows-Gerät

Remote-Zugriff von einem Windows-basierten Gerät mit Kaspersky Security Center Web Console auf ein verwaltetes Linux-Gerät

Remote-Zugriff von einem Windows-basierten Gerät mit Kaspersky Security Center Web Console auf ein verwaltetes Windows-Gerät

Mobile Geräte verwalten

Verwendung von Firebase Cloud Messaging

Integration in die Public-Key-Infrastruktur

Administrationsgruppen verwalten

Administrationsgruppen anlegen

Programme automatisch auf Geräten einer Administrationsgruppe installieren

Administrationsgruppen verschieben

Deleting administration groups

Kaspersky-Anwendungen bereitstellen

Szenario: Kaspersky-Anwendungen bereitstellen

Verwaltungs-Plug-ins für Kaspersky-Anwendungen hinzufügen

Installationspakete

Installationspakete für Kaspersky-Anwendungen herunterladen und erstellen

Installationspakete aus einer Datei erstellen

Autonome Installationspakete erstellen

Einstellungen des Installationspakets des Administrationsagenten

Von Kaspersky Security Center Linux erstellte autonomen Pakete ausführen

Programme mithilfe autonomer Installationspakete installieren

Zweckdienlichkeit des Datenbanken-Updates im Installationspaket der Sicherheitsanwendung

Größenbegrenzung für benutzerdefinierte Installationspakete anpassen

Installationspakete an sekundäre Administrationsserver verteilen

Liste der autonomen Installationspakete anzeigen

Administrationsagent für Linux installieren
- Ein Gerät mit Linux-Betriebssystem für die Installation des Administrationsagenten vorbereiten
- Ein Gerät mit SUSE Linux Enterprise Server 15 für die Installation des Administrationsagenten vorbereiten
- Ein Gerät auf dem Astra Linux im Modus der abgeschlossenen Softwareumgebung ausgeführt wird für die Installation des Administrationsagenten vorbereiten
- Installation des Administrationsagenten auf einem Linux-Betriebssystem mit glibc 2.5 (Legacy-Betriebssystem) vorbereiten
- Installation des Administrationsagenten auf einem Linux-Betriebssystem mit OpenSSH-Version 6.4 (Legacy-Betriebssystem) vorbereiten
- Administrationsagent auf einem Linux-Gerät remote installieren
- Administrationsagent für Linux im Silent-Modus installieren (mit einer Antwort-Datei)
- Administrationsagent für Linux im interaktiven Modus installieren
- Unterstützung des Rollbacks des Dateisystems für Geräte mit Administrationsagent

Administrationsagent für Windows installieren
- Administrationsagent für Windows im interaktiven Modus installieren
- Administrationsagent für Windows im Silent-Modus installieren
- Bereitstellung durch Erstellung und Verteilung eines Geräte-Images
- "Laufwerk klonen"-Modus des Administrationsagenten
- Installationseinstellungen für den Administrationsagenten

Anwendungen mit der Aufgabe zur Remote-Installation installieren
- Über Aufgaben zur Remote-Installation in Kaspersky Security Center Linux
- Eine Anwendung remote installieren
- Remote-Installation von Anwendungen auf macOS-Geräten
- Anwendungen auf sekundären Administrationsservern installieren
- Remote-Installation von Apps auf Geräte mit installiertem Administrationsagenten
- Verwaltung des Neustarts von Geräten in der Aufgabe zur Remote-Installation
- Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center Linux
- Programme im Silent-Modus installieren

Ein Gerät mit dem Betriebssystem macOS für die Remote-Installation des Administrationsagenten vorbereiten

Virtuelle Infrastruktur
- Empfehlungen zur Senkung der Belastung auf den virtuellen Maschinen
- Unterstützung von dynamischen virtuellen Maschinen
- Unterstützung des Kopierens von virtuellen Maschinen

Einstellungen für die Remote-Installation auf Unix-Geräten angeben

Monitoring der Bereitstellung

Kaspersky-Anwendungen starten und beenden

Sicherheitsanwendungen von Drittanbietern ersetzen

Anwendungen oder Software-Updates per Fernzugriff entfernen

Ein Windows-Gerät für die Remote-Installation vorbereiten

Aufgabe zur Remote-Ausführung von Skripten erstellen
- Installationspaket auf Basis einer Manifestdatei erstellen
- Archiv für die Aufgabe zur Remote-Ausführung von Skripten vorbereiten
- Anwendungen mittels Aufgabe zur Remote-Ausführung von Skripten auf Geräten installieren
- Benachrichtigungen und Überwachung für die Aufgabe zur Remote-Ausführung von Skripten konfigurieren

Lizenzierung
Lizenzierung von Kaspersky Security Center Linux
Über den Endbenutzer-Lizenzvertrag
Über die Lizenz
Über das Lizenzzertifikat
Über den Lizenzschlüssel
Anzeigen der Datenschutzrichtlinie
Varianten der Lizenzierung von Kaspersky Security Center
Über die Schlüsseldatei
Über die Bereitstellung von Daten
Über das Abonnement
Kaspersky Security Center Linux aktivieren
Lizenzierung verwalteter Kaspersky-Anwendungen
Lizenzierung der verwalteten Programme
Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
Lizenzschlüssel auf Client-Geräte verteilen
Lizenzschlüssel automatisch verteilen
Informationen zu verwendeten Lizenzschlüsseln anzeigen
Ereignisse bei Überschreitung der Lizenzbeschränkung
Lizenzschlüssel aus der Datenverwaltung löschen
Vereinbarung mit einem Endbenutzer-Lizenzvertrag widerrufen
Lizenzen für Kaspersky-Anwendungen verlängern
Kaspersky Marketplace zum Finden von Kaspersky-Unternehmenslösungen verwenden
Kaspersky-Anwendungen konfigurieren
Szenario: Netzwerkschutz konfigurieren
Geräteorientierte und benutzerorientierte Methode der Sicherheitsverwaltung
Richtlinien einrichten und verwalten: geräteorientierte Herangehensweise
Richtlinien einrichten und verwalten: benutzerorientierte Herangehensweise
Richtlinien und Richtlinienprofile
Über Richtlinien und Richtlinienprofile
Über das Schloss und gesperrte Einstellungen
Vererbung von Richtlinien und Richtlinienprofilen
Hierarchie der Richtlinien
Richtlinienprofile in einer Hierarchie von Richtlinien
Implementierung der Einstellungen auf einem verwalteten Gerät
Richtlinien verwalten
Richtlinienliste anzeigen
Richtlinie erstellen
Allgemeine Richtlinieneinstellungen
Richtlinie ändern
Option zur Vererbung einer Richtlinie aktivieren und deaktivieren
Richtlinien kopieren
Richtlinie verschieben
Richtlinien exportieren
Richtlinien importieren
Erzwungene Synchronisierung
Diagramm für den Status der Richtlinienverteilung anzeigen

Richtlinie nach dem Ereignis "Virenangriff" automatisch aktivieren
Richtlinien löschen
Richtlinienprofile verwalten
Profile einer Richtlinie anzeigen
Priorität eines Richtlinienprofils ändern
Richtlinienprofil erstellen
Richtlinienprofil kopieren
Regeln für die Aktivierung des Richtlinienprofils erstellen
Richtlinienprofil löschen
Richtlinienprofil exportieren und importieren
Richtlinieneinstellungen des Administrationsagenten
Administrationsagent für Windows, Linux und macOS: Vergleich
Vergleich der Einstellungen des Administrationsagenten nach Betriebssystemen
Den ressourcenschonenden Modus des Administrationsagenten aktivieren und deaktivieren
Konfigurieren der Schutzeinstellungen für verwaltete Anwendungen
Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren
Manuelle Konfiguration der Gruppenaufgabe zur Untersuchung des Geräts durch Kaspersky Endpoint Security
Kaspersky Security Network (KSN)
Über KSN
Zugriff auf KSN einrichten
Verwendung von KSN aktivieren und deaktivieren
Die akzeptierte KSN-Erklärung anzeigen
Eine aktualisierte KSN-Erklärung akzeptieren
Feststellen, ob der Verteilungspunkt als KSN-Proxyserver fungiert
Statistiken des KSN-Proxyservers anzeigen
Aufgaben verwalten
Über Aufgaben
Über den Gültigkeitsbereich von Aufgaben
Aufgaben erstellen
Aufgaben manuell starten
Eine Aufgabe für ausgewählte Geräte starten
Aufgabenliste anzeigen
Allgemeine Aufgabeneinstellungen
Aufgaben exportieren
Aufgaben importieren
Assistent zum Ändern der Aufgabenkennwörter starten
Schritt 1. Anmeldedaten angeben
Schritt 2. Auszuführenden Vorgang auswählen
Schritt 3. Ergebnisse anzeigen
Auf dem Administrationsserver gespeicherte Ergebnisse der Aufgabenausführung anzeigen
Anwendungs-Tags
Anwendungs-Tags
Anwendungs-Tag erstellen
Anwendungs-Tag umbenennen
Einer Anwendung Tags zuweisen
Zugewiesene Tags von einer Anwendung entfernen
Anwendungs-Tag löschen

Tools "klscflag" zum Öffnen des Ports 13291 verwenden
Die Kaspersky Industrial CyberSecurity for Networks in der Kaspersky Security Center Web Console registrieren
Benutzer und Benutzerrollen verwalten
Über Benutzerkonten
Über Benutzerrollen
Zugriffsrechte auf Anwendungsfunktionen konfigurieren. Rollenbasierte Zugriffskontrolle
Zugriffsrechte auf Programmfunktionen
Vorkonfigurierte Benutzerrollen
Bestimmten Objekten Zugriffsrechte zuweisen
Zugriffsrechte an Benutzer und Sicherheitsgruppen zuweisen
Benutzerkonto für einen internen Benutzer hinzufügen
Eine Sicherheitsgruppe erstellen
Benutzerkonto eines internen Benutzers bearbeiten
Eine Sicherheitsgruppe bearbeiten
Einem Benutzer oder einer Sicherheitsgruppe eine Rolle zuweisen
Benutzerkonten zu einer internen Sicherheitsgruppe hinzufügen
Benutzer zu Gerätebesitzern ernennen
Benutzer während der Installation des Administrationsagenten zum Gerätebesitzer ernennen
Benutzer nach der Installation des Administrationsagenten zum Linux-Gerätebesitzer ernennen
Benutzer als Gerätebesitzer entfernen
Benutzerkonten-Schutz vor unbefugten Änderungen aktivieren
Konfigurieren Sie die Zwei-Faktor-Authentifizierung
Über die Zwei-Faktor-Authentifizierung für ein Benutzerkonto
Konfigurieren eines geheimen Schlüssels für die Zwei-Faktor-Authentifizierung bei der Anmeldung an der Kaspersky Security Center Web Console
Benutzern die Konfiguration der Zwei-Faktor-Authentifizierung ermöglichen
Zurücksetzen und Löschen eines geheimen Schlüssels für die Zwei-Faktor-Authentifizierung
Benutzerkonten von der Zwei-Faktor-Authentifizierung ausschließen
Name eines Sicherheitscode-Ausstellers bearbeiten
Anzahl der zulässigen Eingabeversuche des Kennworts anpassen
Löschen eines Benutzers oder einer Sicherheitsgruppe
Kennwort eines Benutzerkontos ändern
Benutzerrollen erstellen
Benutzerrollen bearbeiten
Gültigkeitsbereich einer Benutzerrolle bearbeiten
Benutzerrollen löschen
Richtlinienprofile mit Rollen verbinden
Ausdehnen von Benutzerrollen auf sekundäre Administrationsserver
Kennwort des Benutzerkontos ändern
Lokale Administratorrechte entziehen
Kerberos-Domänenauthentifizierung konfigurieren
Datenbanken und Anwendungen von Kaspersky aktualisieren
Szenario: Datenbanken und Programme von Kaspersky regelmäßig aktualisieren
Über das Aktualisieren der Datenbanken, Software-Module und Programme von Kaspersky
Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen
Heruntergeladene Updates prüfen
Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen

Weitere Update-Quellen zu der Aufgabe "Download von Updates in die Datenverwaltung des Administrationsservers" hinzufügen
Programm-Updates genehmigen und ablehnen
Automatische Installation von Updates für Kaspersky Endpoint Security für Windows
Über die Verwendung von Diff-Dateien zum Update von Kaspersky-Datenbanken und Software-Modulen
Funktion zum Herunterladen von Diff-Dateien aktivieren
Updates mittels Verteilungspunkten herunterladen
Datenbanken und Software-Module von Kaspersky auf autonomen Geräten aktualisieren
Überwachung, Berichterstattung und Audit
Szenario: Überwachung und Berichterstattung
Über die Arten der Überwachung und Berichterstattung
Auslösen von Regeln im Smart Training-Modus
Anzeigen und Bestätigen von Funden, die auf Regeln der Adaptiven Kontrolle von Anomalien beruhen
Ausschlüsse aus den Regeln zur Adaptiven Kontrolle von Anomalien hinzufügen
Dashboard und Widgets
Dashboard verwenden
Dem Dashboard Widgets hinzufügen
Widgets im Dashboard verbergen
Widgets auf dem Dashboard verschieben
Größe oder Darstellung von Widgets ändern
Einstellungen von Widgets ändern
Über den Nur-Dashboard-Modus
Nur-Dashboard-Modus konfigurieren
Verwaltungs- und Schutzberichte
Berichte verwenden
Berichtsvorlage erstellen
Eigenschaften von Berichtsvorlagen anzeigen und bearbeiten
Einen Bericht in eine Datei exportieren
Bericht erstellen und anzeigen
Aufgabe zum Berichtsversand anlegen
Berichtsvorlagen löschen
Indikator der Schutzstufe
Es ist Sicherheitsanwendung installiert
Es wird Richtlinie angewendet
Das Update der Antiviren-Datenbanken ist konfiguriert
Das Backup ist konfiguriert
Die Wartung des Administrationsservers ist konfiguriert
Die TLS-Verschlüsselung aktiviert
Ereignisse und Ereignisauswahl
Über Ereignisse in Kaspersky Security Center Linux
Ereignisse der Komponenten von Kaspersky Security Center Linux
Datenstruktur der Beschreibungen von Ereignistypen
Ereignisse des Administrationsservers
Ereignisse des Administrationsservers: Kritisch
Ereignisse des Administrationsservers: Funktionsfehler
Ereignisse des Administrationsservers: Warnung
Ereignisse des Administrationsservers: Information

Ereignisse des Administrationsagenten
Administrationsagent: Ereignisse bei Funktionsfehlern
Ereignisse des Administrationsagenten: Warnung
Ereignisse des Administrationsagenten: Information
Ereignisauswahlen verwenden
Ereignisauswahl erstellen
Ereignisauswahl bearbeiten
Liste mit einer Ereignisauswahl anzeigen
Ereignisauswahl exportieren
Ereignisauswahl importieren
Informationen zu einem Ereignis anzeigen
Ereignisse in eine Datei exportieren
Verlauf eines Objekts aus einem Ereignis heraus anzeigen
Ereignisse löschen
Ereignisauswahl löschen
Speicherdauer für ein Ereignis festlegen
Häufige auftretende Ereignisse blockieren
Über das Blockieren von häufig auftretenden Ereignissen
Das Blockieren häufig auftretender Ereignissen verwalten
Die Blockade häufig auftretender Ereignisse aufheben
Ereignisse auf dem Administrationsserver verarbeiten und speichern
Benachrichtigungen und Gerätestatus
Benachrichtigungen verwenden
Bildschirmbenachrichtigungen anzeigen
Über die Varianten für den Gerätestatus
Wechsel der Statuswerte von Geräten konfigurieren
Einstellungen für das Versenden von Benachrichtigungen anpassen
Verteilung von Benachrichtigungen prüfen
Benachrichtigung über Ereignisse mithilfe einer ausführbaren Datei
Kaspersky-Mitteilungen
Über Kaspersky-Mitteilungen
Einstellungen für die Kaspersky-Mitteilungen festlegen
Kaspersky-Mitteilungen deaktivieren
Informationen über die Erkennung von Bedrohungen anzeigen
Integrationen für die Reaktion auf Alarme
Integration mit Active Directory für die Ausführung von Reaktionsmaßnahmen konfigurieren
Integration mit der Kaspersky Automated Security Awareness Platform konfigurieren
Integration mit Kaspersky Threat Intelligence Portal Sandbox konfigurieren
Alarme nach Attributen gruppieren
Cloud Discovery
Cloud Discovery über das Widget aktivieren
Cloud Discovery-Widget zum Dashboard hinzufügen
Informationen über die Verwendung von Cloud-Diensten anzeigen
Risikostufe eines Cloud-Dienstes
Zugriffs auf unerwünschte Cloud-Dienste blockieren

- Ereignisse in SIEM-Systeme exportieren
  - Ereignisexport in SIEM-Systeme konfigurieren
  - Vorläufige Bedingungen
  - Über den Ereignisexport
  - Über das Konfigurieren des Ereignisexports in ein SIEM-System
  - Über das Exportieren von Ereignissen mittels der Formate CEF und LEEF
  - Ereignisse in das CEF- oder LEEF-Format konvertieren
  - Ereignisse zum Export in SIEM-Systeme im Syslog-Format markieren
    - Ereignisse von Kaspersky-Anwendungen zum Export im Syslog-Format markieren
    - Allgemeine Ereignisse zum Export im Syslog-Format markieren
  - Über das Exportieren von Ereignissen im Syslog-Format
  - Kaspersky Security Center Linux für den Export von Ereignissen in SIEM-Systeme konfigurieren
  - Über das Exportieren von Ereignissen zu Richtlinienänderungen
  - Ereignisse direkt aus der Datenbank exportieren
    - Eine SQL-Abfrage mit dem Tool "klsql2" ausführen
    - Beispielhafte SQL-Abfrage, die mit dem Tool "klsql2" erstellt wurde
    - Name der Datenbank von Kaspersky Security Center Linux anzeigen
  - Exportergebnisse anzeigen
- Umgang mit Objekt-Revisionen
  - Revision einer Richtlinie anzeigen und speichern
  - Richtlinienrevisionen vergleichen
  - Objekte auf eine frühere Version zurück rollen
- Aktive Bedrohungen
  - Unverarbeitete Dateien desinfizieren
  - Unverarbeitete Dateien herunterladen
  - Dateien aus dem Abschnitt "Aktive Bedrohungen" löschen
- Objekte löschen
- Dateien aus Quarantäne und Datei-Backups herunterladen und löschen
  - Dateien aus der Quarantäne und von Datei-Backups herunterladen
  - Über das Entfernen von Objekten aus den Datenverwaltungen der Quarantäne, des Datei-Backups oder der aktiven Bedrohungen
- Die Anwendung über SNMP verwalten
  - Den SNMP-Dienst im Betriebssystem konfigurieren
  - Benachrichtigung per SNMP aktivieren und deaktivieren
  - SNMP in Kaspersky Security Center Linux aktivieren und deaktivieren
  - Werte von Objektkennungen für SNMP

Arbeiten mit Kaspersky Security Center Linux unter der Lizenz für Kaspersky Next XDR Optimum

- Integrationen für die Reaktion auf Alarme
  - Integration mit Active Directory für die Ausführung von Reaktionsmaßnahmen konfigurieren
  - Integration mit der Kaspersky Automated Security Awareness Platform konfigurieren
  - Integration mit Kaspersky Threat Intelligence Portal Sandbox konfigurieren
- Alarme nach Attributen gruppieren

Kaspersky Security Center Web Console in andere Kaspersky-Lösungen integrieren

- Hintergrundverbindung herstellen
- Proxyserver-Verbindung konfigurieren

Ferndiagnose der Client-Geräte
Öffnen des Fensters für die Ferndiagnose
Aktivieren und Deaktivieren der Ablaufverfolgung für Programme
Herunterladen der Protokolldateien eines Programms
Löschen der Protokolldateien
Anwendungseinstellungen herunterladen
Systeminformationen von einem Client-Gerät herunterladen
Ereignisprotokolle downloaden
Starten, Stoppen und Neustarten der Anwendung
Remote-Diagnose für den Kaspersky Security Center Linux Administrationsagenten ausführen und Ergebnisse herunterladen
Ausführen eines Programms auf einem Client-Gerät
Ferndiagnose auf einem Linux-basierten Client-Gerät ausführen
Drittanbieter-Anwendungen und ausführbare Dateien auf den Client-Geräten verwalten
Programmkontrolle zur Verwaltung ausführbarer Dateien verwenden
Liste der auf Client-Geräten gespeicherten ausführbaren Dateien abrufen und anzeigen
Manuell zu erweiternde Programmkategorie erstellen
Programmkategorie mit ausführbaren Dateien von ausgewählten Geräten erstellen
Erstellen einer Programmkategorie mit ausführbaren Dateien aus einem ausgewählten Ordner
Liste der Programmkategorien anzeigen
Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen
Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows konfigurieren
Liste der auf Client-Geräten installierten Anwendungen abrufen und anzeigen
Über Anwendungen von Drittanbietern
Updates für Drittanbieter-Programme installieren
Szenario: Aktualisieren von Software von Drittanbietern
Installationsoptionen der Updates für Drittanbieter-Programme
Einstellungen der Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates
Erstellen der Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"
Informationen zu verfügbaren Updates für Drittanbieter-Programme anzeigen
Liste der verfügbaren Software-Updates in eine Datei exportieren
Genehmigen und Ablehnen der Updates für Drittanbieter-Programme
Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen" erstellen
Regeln für die Update-Installation hinzufügen
Einstellungen der Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen", die nach der Erstellung der Aufgabe angegeben wurden
Drittanbieter-Anwendungen automatisch aktualisieren
Schwachstellen in Drittanbieter-Anwendungen schließen
Über die Suche nach und das Schließen von Software-Schwachstellen
Szenario: Finden und Schließen von Schwachstellen in Programmen von Drittanbietern
Schwachstellen in Drittanbieter-Anwendungen schließen
Erstellen der Aufgabe "Schwachstellen schließen"
Auswählen von Benutzerkorrekturen für Schwachstellen in Programmen von Drittanbietern
Anzeigen von Informationen zu Schwachstellen in Programmen, die auf allen verwalteten Geräten erkannt wurden
Anzeigen von Informationen zu Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden
Statistik über Schwachstellen auf verwalteten Geräten anzeigen

Exportieren der Liste von Schwachstellen in Programmen in eine Datei
Ignorieren von Schwachstellen in Programmen
Installationspaket eines Drittanbieter-Programms aus der Kaspersky-Datenbank erstellen
Einstellungen des Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank anzeigen und anpassen
Einstellungen des Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank
Schwachstellen in einem isolierten Netzwerk schließen
Szenario: Schwachstellen in Drittanbieter-Programmen in einem isolierten Netzwerk beheben
Über das Beheben von Schwachstellen in Programmen von Drittanbietern in einem isolierten Netzwerk
Administrationsserver mit Internetzugang konfigurieren, um Schwachstellen in einem isolierten Netzwerk zu schließen
Isolierte Administrationsserver konfigurieren, um Schwachstellen in einem isolierten Netzwerk zu schließen
Übertragung von Patches und Installation von Updates in einem isolierten Netzwerk
Übertragung von Patches und Installation von Updates in einem isolierten Netzwerk deaktivieren
API-Referenzhandbuch
Bewährte Verfahren für Dienstanbieter
Bereitstellung von Kaspersky Security Center Linux planen
Internetzugriff für den Administrationsserver bereitstellen
Typische Konfiguration von Kaspersky Security Center Linux
Über Verteilungspunkte
Hierarchie des Administrationsservers
Virtuelle Administrationsserver
Bereitstellung und Erstkonfiguration
Installationsempfehlungen für den Administrationsserver
Benutzerkonten für die Dienste des Administrationsservers auf dem Failover-Cluster erstellen
Auswahl des DBMS
Adresse des Administrationsservers angeben
Inaktive Verbindungen aufrechterhalten
Administrationsagent und die Sicherheitsanwendungen bereitstellen
Schutz im Netzwerk eines Kundenunternehmens anpassen
Richtlinie für Kaspersky Endpoint Security manuell konfigurieren
Einstellungen der Richtlinie im Abschnitt "Erweiterter Schutz"
Einstellungen der Richtlinie im Abschnitt "Basisschutz"
Einstellungen der Richtlinie im Abschnitt "Allgemeine Einstellungen"
Einstellungen der Richtlinie im Abschnitt "Konfiguration von Ereignissen"
Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren
Manuelle Konfiguration der Gruppenaufgabe zur Untersuchung des Geräts durch Kaspersky Endpoint Security
Aufgabe "Suche nach Schwachstellen und erforderlichen Updates" planen
Manuelle Konfiguration der Gruppenaufgabe zur Installation von Updates und zum Schließen von Schwachstellen
Aufbau der Struktur von Administrationsgruppen und Zuweisung von Verteilungspunkten
Typische Konfiguration des MSP-Kunden: Einzelbüro
Typische Konfiguration des MSP-Kunden: Mehrere kleine, eigenständige Büros
Richtlinienhierarchie, Verwendung von Richtlinienprofilen
Hierarchie der Richtlinien
Richtlinienprofile
Aufgaben
Verschiebungsregeln für Geräte
Software-Kategorisierung

Verschieben ins Backup und Wiederherstellen der Einstellungen des Administrationsservers
Ein Gerät mit dem Administrationsserver ist ausgefallen
Die Einstellungen des Administrationsservers oder der Datenbank sind beschädigt
Über Verbindungsprofile für mobile Benutzer
Über das Umschalten eines Administrationsagenten auf einen anderen Administrationsserver
Erstellen eines Verbindungsprofils für mobile Benutzer
Remote-Zugriff auf verwaltete Geräte
Verwenden der Option "Verbindung mit Administrationsserver nicht trennen" zur Bereitstellung einer dauerhaften Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver
Über das Überprüfen der Verbindungszeit des Geräts mit dem Administrationsserver
Über erzwungene Synchronisierung
Handbuch zur Skalierung
Zu diesem Handbuch
Berechnungen für die Administrationsserver
Berechnung von Hardwareressourcen für den Administrationsserver
Hardwarevoraussetzungen für DBMS und Administrationsserver
Berechnung des Speicherplatzes in der Datenbank
Berechnung des benötigten Speicherplatzes auf der Festplatte
Berechnung der Anzahl und der Konfiguration der Administrationsserver
Empfehlungen für die Verbindung dynamischer virtueller Maschinen mit Kaspersky Security Center
Berechnungen für Verteilungspunkte und Verbindungs-Gateways
Voraussetzungen für Verteilungspunkte
Anzahl und Konfiguration der Verteilungspunkte bestimmen
Berechnung der Anzahl der Verbindungs-Gateways
Speicherung der Daten zu Ereignissen für Aufgaben und Richtlinien
Bewährte Methoden für einen Administrationsserver, der eine hohe Anzahl von Geräten verwaltet
Besonderheiten und optimale Einstellungen bestimmter Aufgaben
Häufigkeit der Gerätesuche
Aufgaben zum Sichern der Daten des Administrationsservers und zur Pflege von Datenbanken
Gruppenaufgaben zum Update von Kaspersky Endpoint Security
Inventarisierungsaufgabe
Informationen zur Netzwerkauslastung zwischen dem Administrationsserver und den geschützten Geräten
Verbrauch von Datenverkehr bei der Ausführung verschiedener Szenarien
Mittleren Verbrauch von Datenverkehr in 24 Stunden
Bekannte Probleme
Anfrage an den Technischen Support
Technischen Support erhalten
Technischer Support mit Kaspersky CompanyAccount
Dump-Dateien des Administrationsservers abrufen
Informationsquellen über das Programm
Glossar
Administrationsagent
Administrationsgruppe
Administrationsserver
Administrationsserver-Client (Client-Gerät)
Administrator des Anbieters
Administrator von Kaspersky Security Center Linux

Administrator-Arbeitsplatz

Administratorberechtigungen

Aktiver Schlüssel

Anbieter von Antiviren-Schutz

Antiviren-Datenbanken

App Store

Aufgabe

Aufgabe für eine Reihe von Geräten

Aufgabeneinstellungen

Authentifizierungsagent

Backup-Ordner

Broadcast-Domäne

Client-Administrator

Cloud Discovery

Daten-Backup des Administrationsservers

Demilitarisierte Zone (DMZ)

Direkte Anwendungsverwaltung

Ereignis-Datenverwaltung

Ereigniskategorie des Patches

Gerätebesitzer

Geteiltes Zertifikat

Gruppenaufgabe

Gültigkeitsdauer der Lizenz

Home-Administrationsserver

HTTPS

Identitäts- und Zugriffsverwaltung (IAM)

Inkompatible Anwendung

Installationspaket

Interne Benutzer

iOS MDM-Gerät

iOS MDM-Server

JavaScript

Kaspersky Private Security Network (KPSN)

Kaspersky Security Center Linux Webserver

Kaspersky Security Center Operator

Kaspersky Security Center System Health Validator (SHV)

Kaspersky-Update-Server

Konfigurationsprofil

Lightweight Nagent (LWNGT)

Lokale Aufgabe

Lokale Installation

Manuelle Installation

Network Location Awareness (NLA)

Netzwerk-Antiviren-Schutz

Netzwerk-Schutzstatus

Profil

Programmeinstellungen

Provisioning-Profil
Remote-Installation
Richtlinie
Rollengruppe
Schlüsseldatei
Schutzstatus
Schwachstelle
Signifikanz des Ereignisses
SSL
Update
Verbindungs-Gateway
Verfügbares Update
Verteilungspunkt
Verwaltete Geräte
Verwaltungskonsole
Virenangriff
Virtueller Administrationsserver
Wiederherstellung
Wiederherstellung der Daten des Administrationsservers
Zentralisierte Anwendungsverwaltung
Zertifikat des Administrationsservers
Zusätzlicher Lizenzschlüssel (oder Reserve-Lizenzschlüssel)
Informationen über den Code von Drittherstellern
Markenrechtliche Hinweise

Hilfe zu Kaspersky Security Center Linux

Neue Funktionen

- Neuerungen

Hard- und Softwarevoraussetzungen

- Anforderungen an den Administrationsserver
- Anforderungen an die Web Console
- Anforderungen an den Administrationsagenten

Erste Schritte

- Installation
- Schnellstartassistent
- Assistent für die Bereitstellung des Schutzes

Lizenzverwaltung und Aktivierung

- Kaspersky Security Center Linux aktivieren
- Lizenzierung der verwalteten Anwendungen

Bereitstellung und Konfiguration

- Geräte im Netzwerk finden
- Verteilungspunkte und/oder Verbindungs-Gateways anpassen
- Sicherheitsanwendungen von Drittanbietern ersetzen
- Kaspersky-Anwendungen. Zentralisierte Bereitstellung

- Netzwerkschutz konfigurieren
- Kaspersky-Anwendungen. Datenbanken-Update und Update der Programm-Module
- Verbindungsadresse des Administrationsservers konfigurieren
- Migration nach Kaspersky Security Center Linux
- Über das Upgrade von Kaspersky Security Center Linux

Überwachung

- Überwachung und Berichterstattung
- Cloud Discovery

Verwaltung von Client-Geräten

- Remote-Zugriff auf verwaltete Geräte

Schwachstellen- und Patch-Management

- Finden und Schließen von Schwachstellen in Drittanbieter-Programmen

Zusätzliche Funktionen

- Ereignisse in SIEM-Systeme exportieren
- Statistiken des KSN-Proxyservers anzeigen
- Skalierungshandbuch (nur Online-Hilfe)

Neuerungen

Kaspersky Security Center 16.3 Linux

Kaspersky Security Center 16.3 Linux enthält folgende neue Funktionen und Verbesserungen:

- Der Ereignisexport in SIEM-Systeme unterstützt jetzt auch den Export von Ereignissen in das **Kaspersky SIEM** (KUMA).
- Kaspersky Security Center Linux unterstützt jetzt die Lösung Kaspersky Vulnerability Management.
- Um den Empfehlungen des Härtungsleitfadens zu entsprechen, haben wir die Installationskonfiguration von Kaspersky Endpoint Security für Linux optimiert. Dies umfasst die Bereitstellung von KES für Linux sowohl auf Geräten mit Administrationsserver, Web Console und DBMS als auch im Umfeld eines Kaspersky Security Center-Failover-Clusters.
- Während der Installation von Kaspersky Security Center Linux können Sie jetzt ein benutzerdefiniertes Datenbankschema angeben.
- Unter **Überwachung** → **Dashboard** können Sie mithilfe eines Indikators für die Schutzstufe den aktuellen Sicherheitsstatus Ihres Administrationsservers und Ihrer Verteilungspunkte ablesen. Wenn der Indikator gelb oder rot dargestellt wird, sollten Sie bestimmte Maßnahmen ausführen, um das Problem zu beheben und den Status des Indikators auf Grün zu ändern.
- Für die Bereitstellung von Kaspersky Security Center Linux steht jetzt eine vereinfachte Methode zur Verfügung: Die Bereitstellung kann mittels eines Installationsskripts erfolgen.
- Für Legacy-Linux-Systeme mit glib-Version 2.5 ist ein spezielles Programmpaket des Kaspersky-Administrationsagenten verfügbar, das die folgenden alten Betriebssysteme unterstützt:
  - CentOS 5.2
  - CentOS 5.4
  - CentOS 6.4
  - CentOS 6.6
  - Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.4) 64-Bit
- Der Administrationsagent unterstützt jetzt die Betriebssysteme der folgenden neuen Versionen:
  - Microsoft Windows 11 IoT Enterprise, Version 25H2 64-Bit
  - SberOS 3.6.1
  - Ubuntu Server 26.04 LTS
- Die folgenden DBMS werden nicht mehr unterstützt:
  - MySQL 5.7
  - MariaDB 10.1.30

- Verbesserte Benutzerfreundlichkeit:
  - - Verbesserte Filterfunktion für Tabellen mit **Aufgaben** und **Richtlinien** Sie können jetzt mehrere Bedingungen mittels logischem `OR` verknüpfen und einen zusätzlichen neuen Operator verwenden. Mit diesem können Sie für eine Eigenschaft mehrere Werte auswählen und die Zeilen anzeigen lassen, auf die mindestens einer der ausgewählten Werte zutrifft.
  - Im Hauptmenü:
    - - Neuer Abschnitt **Software-Verwaltung** Die folgenden Abschnitte wurden jetzt in die **Software-Verwaltung** verschoben: **Installationspakete**, **Kaspersky-Anwendungen**, **Drittanbieteranwendungen**, **Aktuelle Anwendungsversionen** und **Patch-Management**.
    - - Die Abschnitte **Nicht zugeordnete Geräte** und **Hardware** wurden jetzt in die **Asset-Verwaltung** verschoben.
    - - Die Abschnitte **Aufgaben** und **Datenverwaltung** wurden in die oberste Menüebene verschoben.
    - - Der Abschnitt **Backups der Web-Plug-ins** wird nicht mehr verwendet und wurde aus der Web Console entfernt.

Kaspersky Security Center 16.2 Linux

Übersicht über die neuen Funktionen in Version 16.2. Videodateien

Kaspersky Security Center 16.2 Linux enthält folgende neue Funktionen und Verbesserungen:

- In der Kaspersky Security Center Web Console können Sie jetzt ein Verbindungs-Gateway in der demilitarisierten Zone (DMZ) konfigurieren.

  Um ein Verbindungs-Gateway zu konfigurieren, wählen Sie die Option **Verbindungs-Gateway in der DMZ anhand seiner Adresse verwenden**.

- Der Algorithmus wurde verbessert, sodass die ID des Administrationsagenten (der Parameter `Device ID`) unter Linux erhalten bleibt. Wenn die BIOS-Seriennummer, die Mainboard-Seriennummer, die IDs der Speichermedien oder die MAC-Adresse mit bereits bekannten Werten übereinstimmen, identifiziert der Administrationsserver ein Gerät nach einem Betriebssystem-Update oder einer Änderung der MAC-Adresse als bereits erkanntes Gerät.

- Es wurde die Unterstützung geografisch verteilter Failover-Cluster unter Kaspersky Security Center Linux hinzugefügt, deren Knoten sich in verschiedenen Rechenzentren befinden. In einer geografisch verteilten Cluster-Konfiguration sind alle Komponenten ausfallsicher.

- Sie können jetzt Ereignisse im CEF- oder LEEF-Format in ein SIEM-System exportieren.

- Es wurde die Unterstützung für hochverfügbare PostgreSQL-Cluster mit Patroni für automatisches Failover und für HAProxy zur Lastverteilung hinzugefügt.

- Sie können Richtlinienrevisionen vergleichen. Diese Option ist für Richtlinien der folgenden Komponenten verfügbar: Administrationsserver, Administrationsagent, Kaspersky Endpoint Security für Windows (beginnend ab Version 14.0 des Web-Plug-ins) und Kaspersky Endpoint Security for Mac (beginnend ab Version 12.2.1 Patch A des Web-Plug-ins). Die Liste der unterstützten Kaspersky-Anwendungen wird in zukünftigen Versionen erweitert.

- Die Unterstützung von SNMP wurde hinzugefügt Sie können jetzt den Anwendungen von Drittanbietern Informationen, Statistiken und Ereignisse des Administrationsservers mittels SNMP verfügbar machen.

- Die Windows-Netzwerkabfrage wird jetzt für Windows-basierte Verteilungspunkte unterstützt.

- Für den Administrationsagenten für Linux ist jetzt ein einzelnes Installationspaket verfügbar. Dieses Installationspaket enthält Versionen für verschiedene Paketmanager und CPU-Architekturen. Während der Installation wird die Umgebung automatisch erkannt und das passende Paket des Administrationsagenten installiert.

- Ereignisse enthalten jetzt Informationen über den Initiator von Befehlen, die auf mobilen Geräten ausgeführt wurden.

- Die NSQ-Komponente wurde aus dem Programmpaket der Kaspersky Security Center Web Console entfernt. Der Dienst "KSCWebConsoleMessageQueue.service" wird nicht mehr verwendet und wird nach dem Update der Kaspersky Security Center Web Console entfernt.

- In isolierten Netzwerken erfordert die Erstellung von Installationspaketen für Windows-Geräte den Download zusätzlicher Module von der Kaspersky-Website (die Archive "ri_utils_win32.zip" und "ri_utils_arm64.zip").

- Der Administrationsagent unterstützt jetzt Windows auf 64-Bit-ARM-Architektur. Die Kompatibilität mit verwalteten Anwendungen kann der entsprechenden Hilfedokumentation entnommen werden.

- Kaspersky Security Center Linux unterstützt die Ausführung mit Kaspersky Sandbox.

- Verbesserte Benutzerfreundlichkeit:

  - Sie können jetzt alle Ereignisse auf einmal löschen, die sich in einer Ereignisauswahl oder in Liste mit Geräteereignissen befinden.

    Die Optionen **Alle auswählen** und **Alle auf aktueller Seite auswählen** sind sowohl in der Ereignisauswahl als auch in der Liste der Geräteereignisse verfügbar.

  - Sie können jetzt die Priorität von Verschiebungsregeln manuell festlegen.

    Wenn Sie eine Verschiebungsregel auswählen, wird die Schaltfläche **Priorität ändern** verfügbar, mit der Sie die neue Priorität festlegen können.

- Kaspersky Security Center Linux unterstützt die Ausführung mit Platform V SberLinux OS Server (SLO) 9.6.
- Kaspersky Security Center Linux unterstützt jetzt die folgenden DBMS:
  - MySQL Standard Edition 8.4
  - MySQL Enterprise Edition 8.4
  - PostgreSQL 18
  - Postgres Pro 18 (alle Editionen)
  - Postgres Pro 18 Enterprise (Cluster Built-in High Availability)
- Der Administrationsagent unterstützt jetzt die Betriebssysteme der folgenden neuen Versionen:
  - Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM
  - Platform V SberLinux OS Server (SLO) 9.6

Kaspersky Security Center 16.1 Linux

Kaspersky Security Center 16.1 Linux enthält folgende neue Funktionen und Verbesserungen:

- Zwei-Faktor-Authentifizierung ist jetzt standardmäßig aktiviert. Die globale Option zum Deaktivieren der Zwei-Faktor-Authentifizierung ist nicht mehr verfügbar. Um sicherzustellen, dass sich Benutzer bei der Kaspersky Security Center Web Console und weiterhin OpenAPI-Automatisierungsskripte verwenden können, aktivieren Sie die Zwei-Faktor-Authentifizierung für alle Benutzer, bevor die Aufrüstung.
- Sie können jetzt ein Richtlinienprofil speichern in eine KLPROF-Datei, ohne eine Richtlinie zu exportieren, und verwenden Sie dann diese KLPROF-Datei, um das gespeicherte Profil in die Richtlinie zu importieren.
- Administrationsagent läuft jetzt auf einem Gerät mit ALT OS im Modus „Geschlossene Softwareumgebung“.
- Unterstützung für Kerberos-basierte Domänenauthentifizierung für passwortlose Domänenbenutzer durch Verwendung des SCRIL-Protokoll, Aktivierung der zertifikatsbasierten Einmaliges Anmelden (SSO).
- Verbesserte Benutzerfreundlichkeit:
  - Filterung von Client-Geräten nach Betriebssystemversion und Paketmanager umfasst nun auch Linux-Betriebssystemversionen.
  - Der Mechanismus zur Seitenumbruch für Tabellen in der Kaspersky Security Center Web Console wurde verbessert: Die Standardanzahl der angezeigten Elemente wurde auf 50 erhöht, und die benutzerdefinierte Anzahl der angezeigten Elemente bleibt nun zwischen den Sitzungen erhalten.
  - Kommentare zu den Anwendungskategorien mit denen Sie Beschreibungen von Regeln zum Ein- und Ausschließen von Anwendungen innerhalb einer Kategorie hinzufügen können.
  - Standardmäßig ist die Liste der verfügbaren Installationspakete zeigt nun nur noch Kaspersky-Anwendungsinstallationspakete in der Sprache der Kaspersky Security Center Web Console und in Englisch an.
- Kaspersky Security Center Linux unterstützt die Arbeit mit Kaspersky Endpoint Security für Linux 12.4.

- Kaspersky Security Center Linux unterstützt die Arbeit mit folgendenNeue Betriebssystemversionen:
  - Debian GNU/Linux 13
  - CentOS Stream 10
  - Red Hat Enterprise Linux Server 10.x
- Der Administrationsagent unterstützt jetzt die Betriebssysteme der folgenden neuen Versionen:
  - ALT Workstation 11
  - ALT Server 11
  - ALT Education 11
  - AlterOS 2025
  - SberOS 3.4.0
  - SberOS 3.5.0
  - OSnova 3.*

Kaspersky Security Center 16 Linux

Kaspersky Security Center 16 Linux enthält folgende neue Funktionen und Verbesserungen:

- Die Domänencontroller FreeIPA und ALD Pro werden unterstützt.
- Die Domänenauthentifizierung (Einmaliges Anmelden) wurde Implementierung. Mit der Einmaliges Anmelden-Funktion können Sie die sichere Authentifizierung in Kaspersky Security Center 16 Web Console aktivieren, ohne das Kennwort im Unternehmensnetzwerk erneut eingeben zu müssen. Um die Domänenauthentifizierung zu verwenden, müssen Sie während der Installation von Kaspersky Security Center Web Console die zusätzlichen Parameter in der Antwortdatei angeben.
- Der Kaspersky Security Center 16 Linux Administrationsserver ist nur mit Kaspersky Security Center 16 Web Console kompatibel. Die Verwendung früherer Versionen von Kaspersky Security Center Web Console wird nicht unterstützt.
- Sie können jetzt die Funktionen von Kaspersky Next XDR Optimum unter einer Demolizenz nutzen. Folgende Voraussetzungen müssen dafür erfüllt sein: Sie haben einen sekundären Administrationsserver hinzugefügt, diesen Server unter der Demolizenz aktiviert und den Lizenzschlüssel auf den Geräten bereitgestellt, die durch den sekundären Administrationsserver verwaltet werden.
- Verbesserte Benutzerfreundlichkeit:
  - Die Navigation zwischen den Administrationsgruppen und Administrationsservern wurde vereinfacht: Sie können jetzt von einem einzigen Navigationsbereich aus zwischen den Gruppen und Servern wechseln.
  - Ihre Profileinstellungen werden in den oberen Bereich verschoben.

- Die folgenden Abschnitte des Hauptmenüs wurden umbenannt:
  - Der Abschnitt **Assets (Geräte)** heißt jetzt **Asset-Verwaltung**.
  - Der Abschnitt **Verwaltete Geräte** heißt **Assets (Geräte)**.
  - Der Abschnitt **Direkt-Links** wurde in **Konsolen-Navigation** umbenannt.
- Bei Bedarf kann das Hauptmenü auf Symbole minimiert werden.
- Der Abschnitt **Neuigkeiten von Kaspersky** wird aus dem Abschnitt **Überwachung → Benachrichtigungen** gelöscht.

- Die Filter, die Sie in den Abschnitten **Vorgänge → Patch-Management → Schwachstellen in Programmen** und **Vorgänge → Patch-Management → Software-Updates** auf Tabellen anwenden, wurden jetzt erfolgreich gespeichert und nicht zurückgesetzt.
- Kaspersky Security Center Linux unterstützt die Arbeit mit:
  - Kaspersky NGFW
  - den folgenden Betriebssystemversionen (für die verwalteten Geräte):
    - MosOS 15.5 Arbat
    - Microsoft Windows 11 25H2
    - CentOS 6.4
    - CentOS 6.6

Kaspersky Security Center 15.4 Linux unter einer Lizenz für Kaspersky Next XDR Optimum

Wenn Sie den Administrationsserver unter einer Lizenz für Kaspersky Next XDR Optimum aktiviert und den Lizenzschlüssel für Kaspersky Next XDR Optimum für Ihre verwalteten Anwendungen bereitgestellt haben, können Sie Folgendes tun:

- Alarme nach Attributen gruppieren.
- Integrationen konfigurieren, um auf Bedrohungen zu reagieren.

Kaspersky Security Center 15.4 Linux

Kaspersky Security Center 15.4 Linux enthält eine Reihe neuer Funktionen und Verbesserungen:

- Es stehen jetzt Verbindungsprofile für mobile Benutzer mit Linux-Geräten zur Verfügung. Durch die Verwendung von Verbindungsprofilen können Sie die Regeln für Administrationsagenten auf Linux-Geräten so konfigurieren, dass diese je nach Gerätestandort eine Verbindung zum gleichen oder zu unterschiedlichen Administrationsservern herstellen.
- Es können jetzt Verschlüsselungsschlüssel zwischen Administrationsservern übertragen werden.
- Kaspersky Thin Client wird jetzt unterstützt.

- Der integrierte Hochverfügbarkeits-Cluster von Platform V Pangolin wird jetzt unterstützt.
- Der integrierte Hochverfügbarkeits-Cluster von Postgres Pro wird jetzt unterstützt. Die Knoten dieses DBMS-Clusters werden während der Installation von Kaspersky Security Center Linux im Verbindungs-String angegeben.
- Kaspersky Security Center Linux unterstützt jetzt die folgenden DBMS:
  - Platform V Pangolin 6.5.1
  - Tantor SE 1C für Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.8)
  - Jatoba 5
- Unterstützung für Platform V SberLinux OS Server (SLO), Version 8.10.1, 9.0.1 und 9.5.1.
- Das Archiv "KlAkOAPI.tar.gz" wurde aus der Hilfe entfernt. Das Archiv "KlAkOAPI.tar.gz" befindet sich im Installationsordner von Kaspersky Security Center Linux.
- Die Schaltfläche **Untersuchen** wurde aus dem Abschnitt **Quarantäne** entfernt.
- Da autonome Installationspakete während ihres Downloads erstellt werden, sind die Informationen zu Größe, Datei-Hash und Pfad weder in der Liste der Installationspakete für das autonome Paket des Administrationsagenten noch für alle auf virtuellen Administrationsservern erstellten Pakete verfügbar.

Kaspersky Security Center 15.3 Linux

Kaspersky Security Center 15.3 Linux enthält eine Reihe neuer Funktionen und Verbesserungen:

- Das Tool "klcsngtgui" wurde aus dem Lieferumfang von Kaspersky Security Center Linux entfernt. Mi empfehlen die Verwendung des Tools "klnagchk" anstelle des Tools "klcsngtgui".
- Der Administrationsagent unterstützt jetzt die Betriebssysteme der folgenden neuen Versionen:
  - Microsoft Server 2025
  - Fedora Linux Server 41
  - Fedora Linux Workstation 41
- Kaspersky Security Center Linux unterstützt jetzt die folgenden DBMS:
  - PostgreSQL 17
  - Postgres Pro 17
- Das Kaspersky Update Utility ermöglicht jetzt den Download von ausschließlich erforderlichen Updates für Datenbanken und Software-Module der Sicherheitsanwendungen von Kaspersky. Aktivieren Sie im Eigenschaftenfenster der Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers** die Option **Datei zur Update-Anfrage automatisch herunterladen** und geben Sie den Pfad an, in dem Kaspersky Security Center Linux die Update-Anforderungsdatei mit Informationen über die herunterzuladenden Updates erstellt.
- Es können jetzt die Statistiken zur Nutzung des KSN-Proxyservers angezeigt werden.

- Die anhand des Tools "klbackup" durchgeführte Migration der Daten eines Administrationsservers für Kaspersky Security Center Windows zu Kaspersky Security Center Linux wurde aktualisiert. Sie können jetzt Daten des Administrationsservers, die in einer Microsoft SQL Server-Datenbank gespeichert werden, in PostgreSQL oder Postgres Pro migrieren.

- Die Verbindungsadresse des Administrationsservers kann jetzt konfiguriert werden. Die Verbindungsadresse des Administrationsservers wird beim Erstellen der Installationspakete des Administrationsagenten als Standardadresse und beim Verbinden verwalteter Geräte mit KSN als Adresse des KSN-Proxyservers verwendet.

- Verwaltete Geräte können jetzt zentralisiert neu gestartet werden.

- Informationen über die Benutzer, die aktuell am verwalteten Linux-Gerät angemeldet sind, werden jetzt im Abschnitt **Allgemein** → **Sitzungen** des Fensters mit den Geräteeigenschaften angezeigt.

- Sie können jetzt Fernzugriff auf verwaltete Windows- und Linux-Geräte über die auf den Verwaltete Geräte Administrationsagenten erhalten. Die Verbindung kann über RDP, VNC oder WDS hergestellt werden. Nach der Verbindung mit dem Gerät bekommt der Administrator vollständigen Zugriff auf die Informationen dieses Geräts und kann die auf diesem Gerät installierten Programme verwalten.

- Laden Sie eine Anwendung (oder ein Skript) zur Diagnose auf ein verwaltetes Gerät hoch und führen Sie es aus. Sie können jetzt sowohl das Verzeichnis oder Archiv mit der ausführbaren Datei als auch die ausführbare Datei selbst hochladen. Nachdem die Anwendung erfolgreich ausgeführt wurde, können Sie die Ausführungsergebnisse herunterladen.

- Verbesserte Benutzererfahrung, einschließlich eines neuen Abschnitts mit **Direkt-Links**. Dieser Abschnitt zeigt eine Übersicht des Hauptmenüs an und bietet Ihnen schnellen Zugriff auf alle Abschnitte der Kaspersky Security Center Web Console. Der Abschnitt **Direkt-Links** ist standardmäßig als Startseite eingestellt.

Kaspersky Security Center 15.2 Linux

Kaspersky Security Center 15.2 Linux enthält eine Reihe neuer Funktionen und Verbesserungen:

- Neue Funktionen zur Verwaltung von Kennwörtern interner Benutzerkonten:

  - Sie können jetzt für interne Benutzer beim ersten (oder nächsten) Anmeldeversuch an der Kaspersky Security Center Web Console eine zwingende Änderung des Kennworts konfigurieren.

  - Es wurden neue Option zur Konfiguration des Gültigkeitszeitraums von Kennwörtern für interne Benutzerkonten eingeführt.

- Sie können jetzt die Daten des Administrationsservers für Kaspersky Center Windows sichern und mittels des klbackup-Tools in Kaspersky Security Center Linux wiederherstellen. Die Migration kann ohne Datenverlust zwischen DBMS des gleichen Typs oder zwischen Microsoft SQL Server und MySQL bzw. MariaDB durchgeführt werden.

- Kaspersky Security Center Linux unterstützt jetzt die folgenden DBMS:

  - PostgreSQL 16.x

  - Postgres Pro 16.x

- Kaspersky Security Center Linux unterstützt jetzt bestimmte Arten von PostgreSQL- und Postgres Pro-Clustern.

- Es werden neue Betriebssysteme und neue Betriebssystemversionen unterstützt, einschließlich neuer Versionen von OS MES (Moscow Electronic School), MosTech und MosTech Server.
- Verbesserungen der Benutzerfreundlichkeit:
  - Es wurde die neue Schaltfläche **Speichern** im Fenster für Richtlinieneigenschaften hinzugefügt. Verwenden Sie diese Schaltfläche, wenn Sie die vorgenommenen Änderungen speichern wollen, ohne das Fenster zu schließen.
- Sie können jetzt das Senden von Dateien an Android-Geräte verwalten, zuvor gesendete Dateien löschen und deren Einstellungen im neuen Abschnitt "Apps und Dateien" des Plug-in "Kaspersky Mobile Devices Protection and Management" konfigurieren.
- Sie können jetzt App-Installationspakete und Geräteverwaltungsprofile auf verwaltete mobile Geräte übertragen, ohne diese direkt mit dem Administrationsserver zu verbinden. Dazu dient ein neuer Webserver-Dienst auf einem Verbindungs-Gateway.

Kaspersky Security Center 15.1 Linux

Kaspersky Security Center 15.1 Linux enthält eine Reihe neuer Funktionen und Verbesserungen:

- Kaspersky Security Center Web Console unterstützt jetzt die Verwaltung mobiler Geräte mittels des Plug-ins "Kaspersky Mobile Devices Protection and Management".
- Mittels des Plug-ins für die iOS MDM-Server-Einstellungen können Sie jetzt iOS MDM-Server installieren und konfigurieren, um iOS MDM-Geräte zu verwalten.
- Sie können jetzt die Zertifikate von mobilen Geräten verwalten.
- Kaspersky Endpoint Security für Android wird jetzt unterstützt.
- Kaspersky Security für iOS wird jetzt unterstützt.
- Kaspersky Endpoint Security for Aurora wird jetzt unterstützt.
- Schwachstellen- und Patch-Management für verwaltete Windows-Geräte. Dies betrifft die neue Verwaltung der Updates für Drittanbieter-Programme, die auf verwaltete Windows-Geräte installiert sind, und Schwachstellen beheben, die in diesen Programmen enthalten sind.
- Kaspersky Security Center Linux fragt den Domänencontroller jetzt Seite für Seite ab, anstatt den gesamten Domänencontroller auf einmal abzufragen. Auf diese Weise können Sie Domänencontroller abfragen, die eine große Anzahl von Einträgen enthalten.
- Adaptive Kontrolle von Anomalien. Hierbei handelt es sich um eine Funktion von Kaspersky Endpoint Security für Windows, die mithilfe von Regeln ungewöhnliches Verhalten auf Client-Geräten überwacht und es Ihnen ermöglicht, ungewöhnliche Aktionen zu blockieren.
- Nahtlose Updates der verwalteten Kaspersky-Anwendungen, die auf Windows-Geräten installiert sind, und des Administrationsagenten für Linux. Sie können den Installationsvorgang für Updates verwalten, indem Sie zu installierende Updates genehmigen und zu vermeidende Updates ablehnen.
- Erweiterter Audit für Richtlinien. Sie können sich jetzt den Inhalt einer Richtlinienrevisionen anzeigen lassen und eine Richtlinienrevision in einer Datei speichern. Diese Funktionen sind derzeit nur für die Richtlinien des Administrationsservers und des Administrationsagenten verfügbar.

- Cloud Discovery. Mit dieser neuen Funktion können Sie die Verwendung von Cloud-Diensten auf verwalteten Windows-Geräten überwachen und den Zugriff auf unerwünschte Cloud-Dienste blockieren.

- Der neue Unterabschnitt **Alarme** wurde dem Abschnitt **Überwachung** des Hauptmenüs hinzugefügt. Im Unterabschnitt **Alarme** können Sie Informationen über erkannte Bedrohungen auf den Endpunktgeräten anzeigen. Diese Bedrohungen wurden von den Kaspersky-Sicherheitsanwendungen erkannt.

- Kaspersky Security Center Linux kann jetzt als Komponente der Lösung Kaspersky Managed Detection and Response eingesetzt werden.

- Unterstützung für Kaspersky Security for Virtualization Light Agent.

- Erweiterte Hardware-Inventur für macOS-Geräte. Der Administrationsagent auf einem macOS-Gerät sendet die MAC-Adresse und die Seriennummer des Geräts an den Administrationsserver.

- Sie können jetzt einen Bericht über die Remote-Installation abrufen, wenn Sie Software über benutzerdefinierte Skripte auf den verwalteten Geräten installieren.

- Beim Ausführen mehrerer benutzerdefinierter Skripte auf einem verwalteten Gerät können Sie für jedes Skript eine Priorität festlegen, um die Ausführungsreihenfolge der Skripte zu definieren. Die Skripte werden der Reihe nach entsprechend ihrer Priorität ausgeführt, wobei mit das Skript mit der höchsten Priorität zuerst ausgeführt wird.

- Um die Belastung des Arbeitsspeichers durch Kaspersky Endpoint Security für Linux und durch den Administrationsagenten für Linux zu reduzieren, können Sie für den Administrationsagenten für Linux einen speziellen Betriebsmodus aktivieren. In diesem Modus benötigt der Administrationsagent für Linux bei eingeschränkter Funktionalität weniger Arbeitsspeicher.

- Mit der Aufgabe *Remote-Deinstallation einer Anwendung* können Sie auf den verwalteten Geräten befindliche inkompatible Software deinstallieren.l

- Der Bericht über Netzwerkangriffe beinhaltet jetzt die MAC-Adresse und den Port des angreifenden Geräts.

- Die maximale Länge des Kennworts für interne Benutzer wurde auf 256 Zeichen erhöht.

- Verbesserungen der Benutzerfreundlichkeit, einschließlich:

  - Das Hauptmenü lässt sich personalisieren, indem häufig aufgerufene Abschnitte der Kaspersky Security Center Web Console für einen schnelleren Zugriff zum Abschnitt **Lesezeichen** hinzugefügt werden können.

  - Optimierter Umgang mit Tabellen. Die Standardansicht jeder Tabelle enthält jetzt die am häufigsten verwendeten Spalten. Außerdem können Sie jetzt alle Elemente der aktuellen Seite oder der gesamten Tabelle auswählen sowie die Elemente in der gesamten Tabelle sortieren.

  - Verbesserte Konfiguration der Berichtszustellung. Sie können jetzt bis zu 20 E-Mail-Adressen für die Empfänger des Berichts und den Zeitplan für die Zustellung des Berichts angeben.

- Unterstützung einer Vielzahl an Betriebssystemen und neuen Versionen von Betriebssystemen.

- Ein neues Skalierungshandbuch wurde erstellt und in der Online-Hilfe veröffentlicht.

- Als Ergebnis einer Überprüfung der Benutzeroberfläche wurde ein Problem behoben, das dazu führte, dass der Abschnitt **Remote-Diagnose** im Eigenschaftenfenster des Administrationsservers angezeigt wurde.

- Sie können die Aufgabe *Skripte remote ausführen* erstellen, um auf einem Client-Gerät ein Installationspaket auszuführen und eine Anwendung remote zu installieren.
- Ein Benutzer kann während oder nach der Installation des Administrationsagenten auf einem Linux-Client-Gerät zum Gerätebesitzer ernannt werden.
- Basierend auf dem Gerätebesitzer, der Sicherheitsgruppenmitgliedschaft des Gerätebesitzers und der Rolle des Gerätebesitzers können Sie eine Geräteauswahl oder eine Regel zum Verschieben von Geräten konfigurieren.
- Sie können lokale Administratorrechte von Benutzerkonten entziehen. Dadurch erhalten Sie mehr Kontrolle über die Benutzerkonten. Sie können beispielsweise die lokalen Administratorrechte entziehen, nachdem eine einmalige Zuweisung abgeschlossen wurde.
- Sie können das Kennwort eines lokalen Benutzerkontos ändern. Dies kann nützlich sein, wenn ein Benutzer das Kennwort seines lokalen Benutzerkontos vergisst oder wenn eine geplante Kennwortänderung durchgeführt wird.
- Im Unterabschnitt **Verwaltung von Benutzerzertifikaten** können Sie angeben, welche Stammzertifikate installiert werden sollen. Diese Zertifikate können beispielsweise verwendet werden, um die Authentizität von Websites oder Webservern zu überprüfen.

Kaspersky Security Center 15 Linux

Kaspersky Security Center 15 Linux enthält eine Reihe neuer Funktionen und Verbesserungen:

- Abfrage des Domänencontrollers, mit der Sie sowohl einen Domänencontroller für Microsoft Active Directory als auch für Samba abfragen können. Sie können den Administrationsserver oder einen Verteilungspunkt verwenden, um Microsoft Active Directory abzufragen. Einen Samba-Domänencontroller können Sie nur über einen Verteilungspunkt auf Linux-Basis abfragen. Wenn Sie einen Domänencontroller abfragen, ruft der Administrationsserver oder ein Verteilungspunkt Informationen über die Domänenstruktur, Benutzerkonten, Sicherheitsgruppen und DNS-Namen der Geräte ab, die zur Domäne gehören.
- Kaspersky Security Center Linux unterstützt jetzt die folgenden DBMS:
  - PostgreSQL 15.x
  - Postgres Pro 15.x
- Wenn Sie PostgreSQL oder Postgres Pro als DBMS verwenden, unterstützt Kaspersky Security Center Linux bis zu 50.000 verwaltete Geräte.
- Migration von Kaspersky Security Center Windows auf Kaspersky Security Center Linux. Sie können einen Assistenten ausführen, um die Objekte von Kaspersky Security Center, einschließlich der Aufgaben, Richtlinien und Struktur der Administrationsgruppen, zu migrieren. Anschließend können Sie die importierten verwalteten Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen.
- Kaspersky Security Center Linux unterstützt jetzt die folgenden Kaspersky-Anwendungen:
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Embedded Systems Security für Windows
  - Kaspersky Embedded Systems Security für Linux

- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Agent
- Kaspersky Security for Virtualization Light Agent

- Remote-Diagnose von verwalteten Windows- und Linux-Geräten.
- Die Komponente "Programmkontrolle" wurde verbessert. Sie können jetzt Programmkategorien anhand einer Liste von ausführbaren Dateien innerhalb eines ausgewählten Ordners oder basierend auf einer Kategorie von Kaspersky-Anwendungen erstellen. Anschließend können Sie angeben, ob Sie die Programme der erstellten Kategorie in Ihrer Organisation erlauben oder verbieten möchten.
- Export und Import von Ereignisauswahlen. Der Export einer benutzerdefinierten Ereignisauswahl und ihrer Einstellungen in eine klo-Datei und der anschließende Import der gespeicherten Ereignisauswahl in Kaspersky Security Center Windows oder Kaspersky Security Center Linux sind jetzt möglich.
- Im Bericht über Bedrohungen können Sie jetzt die Entwicklungskette der Bedrohung öffnen, indem Sie auf den Link **Alarm anzeigen** klicken.
- Kaspersky Security Center Linux unterstützt jetzt Cluster-Technologie. Wenn eine Administrationsgruppe Cluster oder Server-Arrays enthält, zeigt die Seite **Assets (Geräte)** zwei Registerkarten an – eine für einzelne Geräte und eine für Cluster und Server-Arrays. Nachdem die verwalteten Geräte als Cluster-Knoten erkannt wurden, wird der Cluster als einzelnes Objekt zur Registerkarte **Cluster und Server-Arrays** hinzugefügt. Die Knoten des Clusters werden zusammen mit anderen verwalteten Geräten auf der Registerkarte **Geräte** angezeigt.
- Für einige Plattformen wurde die Unterstützung durch Kaspersky Security Center Linux eingestellt, da diese Plattformen auch von ihren Herstellern nicht mehr unterstützt werden.

Kaspersky Security Center 14.2 Linux

Kaspersky Security Center 14.2 Linux enthält eine Reihe neuer Funktionen und Verbesserungen:

- In einer Hierarchie der Administrationsserver, kann jetzt ein Linux-basierter Administrationsserver als primärer Server fungieren und Linux- oder Windows-basierte Server verwalten, die als sekundär fungieren.
- Kaspersky Security Center Linux unterstützt jetzt Kaspersky Security Network (KSN), KSN-Proxy-Service, und Kaspersky Private Security Network (KPSN).
- Kaspersky Security Center Linux unterstützt jetzt Kaspersky Endpoint Security für Windows als verwaltete Anwendung.

  Die Remote-Installation des Administrationsagenten für Windows auf Client-Geräten ist nur mit Betriebssystem-Tools über Windows-basierte Verteilungspunkte möglich.
- Daten auf Windows-basierten Geräten können jetzt verschlüsselt werden, um das Risiko eines unbeabsichtigten Verlusts sensibler Informationen und Unternehmensdaten zu verringern, wenn Ihr Laptop oder Ihre Festplatte gestohlen wird oder verloren geht. Diese Funktion wird durch Kaspersky Endpoint Security für Windows implementiert.

- Mit Kaspersky Security Center Linux können Sie sowohl Programmpakete von Kaspersky-Anwendungen als auch Verwaltungs-Web-Plug-Ins direkt in der Benutzeroberfläche von Kaspersky Security Center Linux herunterladen und aktualisieren.

- Standardmäßig werden Informationen über Anwendungen, die auf Linux-basierten und Windows-basierten verwalteten Geräten installiert sind, an den Administrationsserver gesendet.

- Der Zugriff auf Kaspersky-Server wird jetzt automatisch verifiziert. Wenn der Zugriff auf die Server über das systemspezifische DNS nicht möglich ist, verwendet die Anwendung ein öffentliches DNS.

- Sensible Daten, die zwischen dem primären Administrationsserver, den sekundären Administrationsservern und den Administrationsagenten übertragen werden, sind jetzt durch den AES-Verschlüsselungsalgorithmus geschützt.

- Die Benutzerrechte auf einem virtuellen Administrationsserver können unabhängig vom primären Administrationsserver jederzeit konfiguriert werden. Außerdem können Sie den Benutzern primärer Server die Rechte zum Verwalten eines virtuellen Servers zuweisen.

- Kaspersky Security Center Linux unterstützt jetzt die folgenden DBMS:

  - PostgreSQL 13.x

  - PostgreSQL 14.x

  - Postgres Pro 13.x (alle Editionen)

  - Postgres Pro 14.x (alle Editionen)

- Darüber hinaus stehen Ihnen in Kaspersky Security Center Web Console folgende Funktionen zur Verfügung: Export von Richtlinien und Aufgaben in eine Datei, und anschließender Import von Richtlinien und Aufgaben in Kaspersky Security Center Windows oder Kaspersky Security Center Linux.

- Die Option **Keinen Proxyserver verwenden** Option wurde aus den folgenden Aufgaben entfernt:

  - *Download von Updates in die Datenverwaltung des Administrationsservers*

  - *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*

Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux enthält eine Reihe neuer Funktionen und Verbesserungen:

- Antiviren-Datenbanken für Kaspersky-Sicherheitsanwendungen können jetzt neben der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* auch durch die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* heruntergeladen werden.

- Die Antiviren-Datenbanken und Anwendungsmodule auf den verwalteten Geräten können über einen Administrationsserver oder über Verteilungspunkte verbreitet und aktualisiert werden. Sie können ein optimales Update-Schema für Ihr Unternehmen auswählen, um die Belastung des Administrationsservers zu reduzieren und den Datenverkehr im Unternehmensnetzwerk zu optimieren.

- Kaspersky Security Center Linux lädt von den Kaspersky-Update-Servern nur die Updates herunter, die von den Kaspersky-Sicherheitsanwendungen angefordert werden. Dadurch wird die Größe der heruntergeladenen Daten reduziert.

- Für den Download von Antiviren-Datenbanken und Programm-Modulen können Sie jetzt die Funktion für Diff-Dateien verwenden. Eine Diff-Datei beschreibt den Unterschied zwischen zwei Versionen der Datei einer Datenbank oder eines Programm-Moduls. Die Verwendung von Diff-Dateien entlastet den Datenverkehr in Ihrem Unternehmen Netzwerk, da Diff-Dateien weniger Platz einnehmen als die vollständigen Dateien der Datenbanken und Software-Module.

- Die Aufgabe *Update-Prüfung* wurde hinzugefügt. Mit dieser Aufgabe können Sie die heruntergeladenen Updates automatisch auf Funktionsfähigkeit und Fehler überprüfen, bevor Sie die Updates auf den verwalteten Geräten installieren.

- Kaspersky Security Center Linux unterstützt jetzt Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 als verwaltete Anwendung.

Behobene Probleme

Die folgende Tabelle listet alle Probleme auf, die in früheren Versionen Kaspersky Security Center Linux gefunden wurden, und welche in der aktuellen Version behoben wurden.

Liste der Probleme, die in Kaspersky Security Center Linux 16.3 behoben wurden

Version von Kaspersky Security Center Linux in der das Problem erstmals auftrat	Problem-ID	Problembeschreibung
16.2	9959974	Es wurde ein Problem behoben, bei dem im Fenster mit den Geräteeigenschaften die Registerkarte **Ereignisse** die Option **Alle auswählen** beinhaltete, welche alle Ereignisse aus der Datenbank des Administrationsservers löschen konnte.
16.2	9392997	Es wurde ein Problem behoben, durch das dem Ereignisprotokoll nach einer erfolgreichen Abfrage eines ALD Pro- oder FreeIPA-Domänencontrollers eine Fehlermeldung hinzugefügt wurde.
16.2	9504495	Es wurde ein Problem behoben, das zu einer falschen Zuweisung eines Benutzers führen konnte, wenn ein Gerätebesitzer über die Parameter des Installationspakets des Administrationsagenten zugewiesen wurde.
16.1	9316206	Es wurde ein Problem behoben, durch das Schaltflächen auf der Registerkarte **Zwei-Faktor-Authentifizierung** verschwinden konnten, wenn Sie den Browser nach dem Öffnen der Registerkarte aktualisierten.
16.1	7555541	Es wurde ein Problem behoben, durch das die Anmeldung an der Web Console fehlschlagen konnte, wenn Sie beim Erstellen der Aufgabe *Kennwort des Benutzerkontos ändern (nur Linux)* die Option **Dies ist ein Einmalkennwort (der Benutzer muss das Kennwort nach dem ersten Anmelden ändern)** aktivierten.
15.5	755788	Es wurde ein Problem behoben, bei dem die Aufgabe *Kennwort des Benutzerkontos ändern* möglicherweise nicht korrekt funktionierte, wenn SELinux auf dem Benutzergerät aktiviert war.
16.2	9603496	Es wurde ein Problem behoben, durch das Sie den Administrationsagenten auf dem Gerät mit dem Administrationsserver installieren mussten, um Diagnoseinformationen zu diesem Gerät zu erhalten.

Liste der Probleme, die in Kaspersky Security Center Linux 16.2 behoben wurden

Version von Kaspersky Security Center Linux in der das Problem erstmals auftrat	Problem-ID	Problembeschreibung
15.1	10071566	Es wurde ein Problem behoben, bei dem Änderungen an einem Aufgabenzeitplan nicht an die verwalteten Geräte übertragen wurden, wenn im Zeitplan die Einstellung "Nach Wochentagen" verwendet wurde.
15.4	9067754	Es wurde ein Problem behoben, bei dem neue Ereignisse nach der Aktualisierung des Plug-ins von Kaspersky Mobile Devices Protection and Management fälschlicherweise in einer zuvor erstellten Richtlinie angezeigt wurden.
16	9329729	Es wurde ein Problem behoben, bei dem nach dem Upgrade von Kaspersky Security Center Linux von Version 16 auf Version 16.1 ein Fehler im Kaspersky-Ereignisprotokoll angezeigt wurde, wenn vor dem Upgrade für bestimmte Benutzer die Zwei-Faktor-Authentifizierung konfiguriert war.
16.1	9256000	Es wurde ein Problem behoben, bei dem keine Informationen über verwaltete Anwendungskomponenten verfügbar waren, wenn der Administrationsagent unter Microsoft Windows XP installiert ist.
16.1	9251629	Es wurde ein Problem behoben, bei dem bei Anmeldung an der Kaspersky Security Center Web Console einige erforderliche HTTP-Response-Header nicht hinzugefügt wurden.

Über Kaspersky Security Center Linux

Dieser Abschnitt informiert über die Konzeption, die wichtigsten Funktionen, die Programmkomponenten und Vorgehensweisen zum Erwerb von Kaspersky Security Center Linux.

Kaspersky Security Center Linux (im Weiteren auch als "Kaspersky Security Center" bezeichnet) wurde entwickelt, um den Schutz von Client-Geräten bereitzustellen und zu verwalten, indem ein Linux-basierter Administrationsserver verwendet wird.

Mit Kaspersky Security Center Linux können Sie Kaspersky-Sicherheitsanwendungen auf Geräten in einem Unternehmensnetzwerk installieren, Untersuchungs- und Update-Aufgaben per Fernzugriff ausführen und die Sicherheitsrichtlinien verwalteter Anwendungen verwalten. Als Administrator verfügen Sie über ein umfassendes Dashboard, das einen Überblick über den Status der Unternehmensgeräte, ausführliche Berichte und Schutzrichtlinien mit detaillierten Einstellungen bereitstellt.

Kaspersky Security Center Linux hat einen anderen Funktionsumfang als Kaspersky Security Center mit einem Windows®-basierten Administrationsserver.

Kaspersky Security Center Linux ist für Administratoren von Unternehmensnetzwerken und für Mitarbeiter gedacht, die für die Sicherheit von Geräten in Unternehmen verantwortlich sind.

Kaspersky Security Center bietet Ihnen folgende Möglichkeiten:

- Eine Hierarchie der Administrationsserver erstellen, um das eigene Unternehmensnetzwerk sowie Netzwerke entfernter Standorte bzw. Kundenunternehmen verwalten zu können.

  Mit *Kundenunternehmen* bezeichnet man Unternehmen, deren Antiviren-Schutz von Dienstanbietern gewährleistet wird.

- Eine Hierarchie der Administrationsgruppen erstellen, um eine Gruppe von bestimmten Client-Geräten als Ganzes zu verwalten.

- Antiviren-Schutz verwalten, der auf Kaspersky-Anwendungen basiert.

- Anwendungen von Kaspersky und anderen Softwareanbietern per Fernzugriff installieren.

- Zentralisierte Verteilung von Lizenzschlüsseln für Kaspersky-Anwendungen an die Client-Geräte, Überwachung der Verwendung von Lizenzschlüsseln, Verlängerung von Lizenzen.

- Statistiken und Berichte über die Ausführung von Anwendungen und Geräten abrufen.

- Benachrichtigungen über kritische Ereignisse bei der Ausführung von Kaspersky-Anwendungen empfangen.

- Verschlüsselung von Informationen, die auf Festplatten von Windows-basierten Geräten und Wechseldatenträgern gespeichert sind verwalten.

- Benutzerzugriff auf verschlüsselte Daten auf Windows-basierten Geräten verwalten.

- Inventarisierung der mit dem Unternehmensnetzwerk verbundenen Hardware durchführen.

- Dateien, die von den Sicherheitsanwendungen in die Quarantäne oder ins Backup verschoben wurden, sowie Dateien, deren Verarbeitung durch die Sicherheitsanwendungen aufgeschoben wurde, zentral verwalten.

Sie können Kaspersky Security Center Linux direkt bei Kaspersky (beispielsweise auf https://www.kaspersky.de) oder über unsere Partnerunternehmen erwerben.

Wenn Sie Kaspersky Security Center Linux direkt über Kaspersky erwerben, können Sie die Anwendung von unserer Website herunterladen. Sie erhalten die zur Anwendungsaktivierung erforderlichen Informationen per E-Mail, nachdem der Eingang Ihres Rechnungsbetrags verarbeitet wurde.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Lieferumfang

Auf der Kaspersky-Website können Sie alle erforderlichen Installationspakete der Anwendung herunterladen.

Der Lieferumfang von Kaspersky Security Center Linux umfasst die folgenden Dateien:

Administrationsserver für Kaspersky Security Center Linux:

- Administrationsserver zur Installation auf einem Gerät mit Debian-basierten Betriebssystem:
  ksc64_16.2.0-<Build-Nummer>_amd64.deb
- Administrationsserver zur Installation auf einem Gerät mit Red Hat Enterprise Linux-basierten Betriebssystem:
  ksc64-16.2.0-<Build-Nummer>.x86_64.rpm

Kaspersky Security Center Web Console:

- Web Console zur Installation auf einem Gerät mit Debian-basierten Betriebssystem:
  ksc-web-console-16.2.<Build-Nummer>.x86_64.deb
- Web Console zur Installation auf einem Gerät mit Red Hat Enterprise Linux-basierten Betriebssystem:
  ksc-web-console-16.2.<Build-Nummer>.x86_64.rpm

Administrationsagent für Windows:

- Administrationsagent zur Installation auf Geräten mit x86-32- oder x64-Architektur:
  ksc_16_16.2.0.<Build-Nummer>_NetAgent_<Sprache>.zip
- Administrationsagent zur Installation auf Geräten mit Arm-Architektur:
  klnagent_winarm64-16.2.0.<Build-Nummer>-win_<Sprache>.zip
- Tool zur Remote-Installation des Administrationsagenten auf einem Gerät mit Red Hat Enterprise Linux-basierten Betriebssystem:
  ri_utils_arm64.zip
- Tool zur Remote-Installation des Administrationsagenten auf Geräten mit 32-Bit- oder 64-Bit-Betriebssystem:
  ri_utils_win32.zip

Administrationsagent für Linux:

- Administrationsagent zur Installation auf einem Gerät mit Debian-basierten Betriebssystem:
  klnagent64_16.2.0-<Build-Nummer>_<Architektur>.deb

- Administrationsagent zur Installation auf einem Gerät mit Red Hat Enterprise Linux-basierten Betriebssystem:

  klnagent64-16.2.0-<Build-Nummer>_<Architektur>.rpm

- Dateien zur Remote-Installation des Administrationsagenten auf einem Gerät mit Debian-basierten Betriebssystem:

  klnagent-<Architektur>-16.2.0.<Build-Nummer>-deb_<Sprache>.tar.gz

- Dateien zur Remote-Installation des Administrationsagenten auf einem Gerät mit Red Hat Enterprise Linux-basierten Betriebssystem:

  klnagent-<Architektur>-16.2.0.<Build-Nummer>-rpm_<Sprache>.tar.gz

- All-in-one-Programmpaket des Administrationsagenten für Linux:

  klnagent-ALL-16.2.0.<Build-Nummer>-ALL_<Sprache>.tar.gz

  Das All-in-one-Programmpaket kann nützlich sein, wenn Sie viele Client-Geräte mit unterschiedlicher CPU-Architektur und verschiedenen Linux-basierten Betriebssystemen betreiben. Die erforderlichen Versionen der Administrationsagenten werden automatisch für die weitere Installation auf den Geräten ausgewählt.

Web-Plug-in von Kaspersky Endpoint Detection and Response Optimum:

- signed_irp.zip

  Sie können das Web-Plug-in nur aus dem Repository von Programmpaketen für Anwendungen zur Remote-Installation herunterladen.

Wenn Ihnen die Auswahl eines Installationspakets für den Administrationsagenten unter Linux Schwierigkeiten bereitet, können Sie diesen Artikel lesen: So wählen Sie das Installationspaket des Administrationsagenten für Linux aus.

Hard- und Softwarevoraussetzungen

- Anforderungen an den Administrationsserver
- Anforderungen an die Web Console
- Anforderungen an den Administrationsagenten

Weitere Informationen über die Versionsanforderungen an Android und iOS zur Bereitstellung des Schutzes und die Verwaltung mobiler Geräte finden Sie in der Hilfe zu Kaspersky Security für mobile Endgeräte und Kaspersky Secure Mobility Management.

Anforderungen an den Administrationsserver

Mindestvoraussetzungen an die Hardware:

- CPU mit einer Taktfrequenz von 2. GHz oder höher und 2 Kernen.
- RAM: 6 GB.

  Auf dem Gerät mit dem installierten Administrationsserver müssen Sie die Verwendung der Swap-Datei aktivieren. Die Swap-Datei muss mindestens 1,5-mal größer sein als der Arbeitsspeicher.
- Verfügbarer Speicherplatz: 10 GB sind für den Ordner erforderlich, der die Daten des Administrationsservers enthält (/var/opt/kaspersky/klnagent_srv).

Es wird empfohlen, nach der Installation des Administrationsservers auf dem Gerät ebenfalls Kaspersky Endpoint Security für Linux zu installieren.
Für die gleichzeitige Installation müssen mindestens 300 IOPS verfügbar sein. Darüber hinaus erhöhen sich die Anforderungen an den Administrationsserver um 1,5 GB RAM und 15% CPU-Leistung.
Weitere Informationen zu den Hardware-Anforderungen von Kaspersky Endpoint Security finden Sie in der Hilfe zu Kaspersky Endpoint Security für Linux.

Die folgenden Betriebssysteme werden unterstützt:

Damit die Prozesse im Betriebssystem untereinander kommunizieren können, muss die Loopback-Schnittstelle verfügbar sein.

- Debian GNU/Linux 12 (Bookworm) 64-Bit
- Debian GNU/Linux 13 (Trixie) 64-Bit
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-Bit
- Ubuntu Server 24.04 LTS (Noble Numbat) 64-Bit
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64-Bit
- CentOS Stream 9 64-Bit
- CentOS Stream 10 64-Bit
- Red Hat Enterprise Linux Server 7.x 64-Bit
- Red Hat Enterprise Linux Server 8.x 64-Bit
- Red Hat Enterprise Linux Server 9.x 64-Bit
- Red Hat Enterprise Linux Server 10.x 64-Bit
- SUSE Linux Enterprise Server 12 (alle Service Packs) 64-Bit

- SUSE Linux Enterprise Server 15 (alle Service Packs) 64-Bit
- Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.6) 64-Bit
- Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.7) 64-Bit
- Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.8) 64-Bit
- Astra Linux Special Edition RUSB.10015-16 (Release 1) (operatives Update 1.6) 64-Bit
- Astra Linux Special Edition RUSB.10015-17 (operatives Update 1.7.3) 64-Bit
- Astra Linux Special Edition RUSB.10015-03 (operatives Update 7.6) 64-Bit
- Astra Linux Special Edition RUSB.10015-37 (operatives Update 7.7) 64-Bit
- Astra Linux Common Edition (operatives Update 2.12) 64-Bit
- ALT SP Server 10 64-Bit
- ALT SP Workstation 10 64-Bit
- Oracle Linux 7 64-Bit
- Oracle Linux 8 64-Bit
- Oracle Linux 9 64-Bit
- Plattform V SberLinux OS Server (SLO) 8.10.1 64-Bit
- Plattform V SberLinux OS Server (SLO) 9.5.1 64-Bit
- Plattform V SberLinux OS Server (SLO) 9.6 64-Bit
- Platform V SberLinux OS Server (SLO) 9.7 64-Bit
- RED OS 7.3 Server 64-Bit
- RED OS 7.3 Certified Edition 64-Bit
- RED OS 8 64-Bit
- ROSA COBALT 7.9 64-Bit
- M OS (Moscow Electronic School) 12 Server 64-bit
- Mostech Server 64-Bit
- MosOS 15.5 Arbat 64-Bit

Es wird die Verwendung des EXT4-Dateisystems mit dessen Standardeinstellungen empfohlen.

Die folgenden Datenbankserver werden unterstützt (Installation auf einem anderen Gerät möglich):

- MySQL Standard Edition 8.0 (Release 8.0.20 und höher) 32-Bit/64-Bit
- MySQL Enterprise Edition 8.0 (Release 8.0.20 und höher) 32-Bit/64-Bit
- MySQL Standard Edition 8.4 32-Bit/64-Bit
- MySQL Enterprise Edition 8.4 32-Bit/64-Bit
- MariaDB 10.3 (Build 10.3.22 und höher) 32-Bit/64-Bit
- MariaDB 10.4 (Build 10.4.20 und höher) 32-Bit/64-Bit
- MariaDB 10.5 (Build 10.5.27 und höher) 32-Bit/64-Bit
- MariaDB 10.6 (Build 10.6.20 und höher) 32-Bit/64-Bit
- MariaDB 10.11 (Build 10.11.10 und höher) 32-Bit/64-Bit
- MariaDB Galera Cluster 10.3 32-Bit/64-Bit mit InnoDB Storage Engine
- PostgreSQL 13.x 64-Bit
- PostgreSQL 14.x 64-Bit
- PostgreSQL 15.x 64-Bit
- PostgreSQL 15.x 64-Bit (Cluster Corosync/Pacemaker)
- PostgreSQL 16.x 64-Bit
- PostgreSQL 17 64-Bit
- PostgreSQL 18 64-Bit
- Postgres Pro 13.x 64-Bit (alle Editionen)
- Postgres Pro 14.x 64-Bit (alle Editionen)
- Postgres Pro 15.x 64-Bit (alle Editionen)
- Postgres Pro 15.x 64-Bit (Cluster Corosync/Pacemaker)
- Postgres Pro 16.x 64-Bit (alle Editionen)
- Postgres Pro 16.x Enterprise 64-Bit (Cluster Built-in High Availability)
- Postgres Pro 17 64-Bit (alle Editionen)
- Postgres Pro 17 Enterprise 64-Bit (Cluster Built-in High Availability)
- Postgres Pro 18 64-Bit (alle Editionen)
- Postgres Pro 18 Enterprise 64-Bit (Cluster Built-in High Availability)

- Platform V Pangolin 6.5.1 64-Bit
- Plattform V Pangolin 6.5.1 64-Bit (Cluster Built-in High Availability)
- Jatoba 4 64-Bit
- Jatoba 5 64-Bit
- Tantor SE 1C 64-Bit

Hochverfügbare PostgreSQL-Cluster werden unterstützt. Ausführliche Informationen dazu finden Sie im folgenden Artikel: Ein hochverfügbares DBMS-Cluster für die Arbeit mit Kaspersky Security Center Linux vorbereiten.

Ausführliche Informationen zu den unterstützten Virtualisierungsplattformen finden Sie in der Online-Hilfe zu Kaspersky Security for Virtualization Light Agent.

Anforderungen an die Web Console

Server der Kaspersky Security Center Web Console

Hardwaremindestvoraussetzungen:

- CPU: 2 Kerne, Taktfrequenz 2,5 GHz.
- RAM: 4 GB.
- Verfügbarer Speicherplatz: 40 GB sind für den Ordner erforderlich, der die Daten der Web Console enthält (/var/opt/kaspersky).

Es wird empfohlen, nach der Installation von Kaspersky Security Center Web Console ebenfalls Kaspersky Endpoint Security für Linux auf diesem Gerät zu installieren. Weitere Informationen zu den Hardware-Anforderungen von Kaspersky Endpoint Security finden Sie in der Hilfe zu Kaspersky Endpoint Security für Linux.

Eines der folgenden Betriebssysteme (**nur 64-Bit-Versionen**):

> Damit die Prozesse im Betriebssystem untereinander kommunizieren können, muss die Loopback-Schnittstelle verfügbar sein.

- Debian GNU/Linux 12 (Bookworm)
- Debian GNU/Linux 13
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- Ubuntu Server 24.04 LTS (Noble Numbat)
- Ubuntu Server 26.04 LTS (Resolute Raccoon) 64-Bit
- CentOS Stream 9

- CentOS Stream 10
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.x
- Red Hat Enterprise Linux Server 10.x
- SUSE Linux Enterprise Server 12 (alle Service Packs)
- SUSE Linux Enterprise Server 15 (alle Service Packs)
- Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.6)
- Astra Linux Special Edition RUSB.10015-16 (Release 1) (operatives Update 1.6)
- Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.7)
- Astra Linux Special Edition RUSB.10015-17 (operatives Update 1.7.3)
- Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.8)
- Astra Linux Special Edition RUSB.10015-03 (operatives Update 7.6)
- Astra Linux Special Edition RUSB.10015-37 (operatives Update 7.7)
- Astra Linux Common Edition (operatives Update 2.12)
- ALT SP Server 10
- ALT SP Workstation 10
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- Platform V SberLinux OS Server (SLO) 8.10.1
- Platform V SberLinux OS Server (SLO) 9.5.1
- Plattform V SberLinux OS Server (SLO) 9.6 64-Bit
- Platform V SberLinux OS Server (SLO) 9.7 64-Bit
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition
- RED OS 8
- ROSA COBALT 7.9

- M OS (Moscow Electronic School) 12 Server
- Mostech Server
- MosOS 15.5 Arbat

Ausführliche Informationen zu den unterstützten Virtualisierungsplattformen finden Sie in der Online-Hilfe zu Kaspersky Security for Virtualization Light Agent.

Client-Geräte

Für die Nutzung von Kaspersky Security Center Web Console auf einem Client-Gerät ist nur ein Browser erforderlich.

Die minimale Bildschirmauflösung beträgt 1366 x 768 Pixel.

Die Hard- und Softwarevoraussetzungen für das Gerät entsprechen den Anforderungen des Browsers, der für die Arbeit mit Kaspersky Security Center Web Console verwendet wird.

Browser:

- Google Chrome 149.0.7827.115 oder höher
- Microsoft Edge 149.0.4022.62 oder höher
- Safari 18.6 (20621.3.11.11.3) unter macOS
- Yandex Browser 26.4.4.799 oder höher
- Mozilla Firefox Extended Support Release 140.11.0 oder höher

Anforderungen an den Administrationsagenten

Hardwaremindestvoraussetzungen:

- CPU mit einer Taktfrequenz von 1 GHz oder höher. Für 64-Bit-Betriebssysteme beträgt die minimale Taktfrequenz des Prozessors 1.4 GHz.
- RAM: 512 MB.
- Freier Speicherplatz auf dem Datenträger: 1 GB.

Softwarevoraussetzung für Linux-basierte Geräte: Der Perl-Sprachinterpreter Version 5.10 oder höher muss installiert sein.

Administrationsagent. Unterstützte Plattformen

Betriebssysteme. Workstations mit Microsoft Windows	Microsoft Windows Embedded POSReady 2009 mit dem aktuellsten Service Pack, 32-Bit Microsoft Windows Embedded 7 Standard mit Service Pack 1 32-Bit/64-Bit Microsoft Windows Embedded 8.1 Industry Pro 32-Bit/64-Bit Microsoft Windows 10 Enterprise 2015 LTSB 32-Bit/64-Bit Microsoft Windows 10 Enterprise 2016 LTSB 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise 2015 LTSB 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise 2016 LTSB 32-Bit/64-Bit Microsoft Windows 10 Enterprise 2019 LTSC 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise Version 1703, 1709, 1803, 1809 32-Bit/64-Bit Microsoft Windows 10 20H2, 21H2 IoT Enterprise 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise Version 1909 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise LTSC 2021 32-Bit/64-Bit Microsoft Windows 10 IoT Enterprise Version 1607 32-Bit/64-Bit Microsoft Windows 10 TH1 (Juli 2015) Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 TH2 (November 2015) Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS1 (August 2016) Home/Pro/Pro für Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS2 (April 2017) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS3 (Fall Creators Update, v1709) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS4 (Update vom April 2018, 17134) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS5 (Oktober 2018) Home/Profi/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 RS6 (Mai 2019) Home/Profi/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 10 19H1, 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 20H1 (Update vom Mai 2020) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 20H2 (Update vom Oktober 2020) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 20H1 (Update vom Mai 2020) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 10 21H2 (Update vom Oktober 2021) Home/Pro/Pro für Workstations/Enterprise/Bildung 32-Bit/64-Bit Microsoft Windows 10 22H2 (Update vom Oktober 2023) Home/Pro/Pro for Workstations/Enterprise/Education 32-Bit/64-Bit Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education ARM 64-Bit Microsoft Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 11 IoT Enterprise, Version 25H2 64-Bit Microsoft Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 11 25H2 Home/Pro/Pro for Workstations/Enterprise/Education 64-Bit Microsoft Windows 8.1 Pro/Enterprise 32-Bit/64-Bit Microsoft Windows 8 Pro/Enterprise 32-Bit/64-Bit Microsoft Windows 7 Professional/Enterprise/Ultimate/Home Basic/Premium mit Service Pack 1 und höher, 32-Bit/64-Bit Microsoft Windows XP Professional mit Service Pack 2 32-Bit/64-Bit (nur von Administrationsagent Version 10.5.1781 unterstützt) Microsoft Windows XP Professional mit Service Pack 3 und höher, 32-Bit (unterstützt vom Administrationsagenten in Version 14.0.0.20023; erfordert das Sicherheitsupdate für Windows XP KB2868626) Microsoft Windows XP Professional for Embedded Systems mit Service Pack 3 32-Bit (unterstützt vom Administrationsagenten in Version 14.0.0.20023)

Betriebssysteme. Server mit Microsoft Windows	Microsoft Windows MultiPoint Server 2011 Standard/Premium 64-Bit Microsoft Windows Server 2003 SP1 32-Bit/64-Bit (unterstützt nur durch den Administrationsagenten in Version 10.5.1781, die Sie über den Technischen Support anfordern können) Microsoft Windows Server 2003 SP2 Standard/Enterprise 32-Bit/64-Bit (unterstützt nur durch den Administrationsagenten in Version 10.5.1781) Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 32-Bit/64-Bit (unterstützt nur durch den Administrationsagenten in Version 10.5.1781) Microsoft Windows Server 2008 Foundation mit Service Pack 2 32-Bit/64-Bit Microsoft Windows Server 2008 Standard/Enterprise/Datacenter mit Service Pack 2 32-Bit/64-Bit Microsoft Windows Server 2008 R2 Datacenter/Enterprise/Foundation/Standard mit Service Pack 1 und höher, 64-Bit Microsoft Windows Server 2012 Server Core/Datacenter/Essentials/Foundation/Standard 64-Bit Microsoft Windows Server 2012 R2 Server Core/Datacenter/Essentials/Foundation/Standard 64-Bit Microsoft Windows Server 2016 Datacenter/Standard/Server Core (Installation Option) (LTSB) 64-Bit Microsoft Windows Server 2019 Standard/Datacenter/Core 64-Bit Microsoft Windows Server 2019 RS5 Essentials/Standard 64-Bit Microsoft Windows Server 2022 Standard/Datacenter/Core 64-Bit Microsoft Windows Server 2025 Standard/Datacenter/Core 64-Bit Microsoft Windows Server 2022 21H2 Standard/Datacenter 64-Bit Microsoft Windows Storage Server 2019 64-Bit Microsoft Windows Small Business Server 2011 Standard 64-Bit Microsoft Windows Small Business Server 2011 Essentials 64-Bit Microsoft Windows Small Business Server 2011 Premium Add-on 64-Bit

Betriebssysteme. Linux	Debian GNU/Linux 10.x (Buster) 32-Bit/64-Bit Debian GNU/Linux 11.x (Bullseye) 32-Bit/64-Bit Debian GNU/Linux 12 (Bookworm) 32-Bit/64-Bit Debian GNU/Linux 13 (Trixie) 64-Bit Ubuntu Server 10.04 LTS (Lucid Lynx) 32-Bit/64-Bit Ubuntu Server 16.04 LTS (Xenial Xerus) 32-Bit/64-Bit Ubuntu Server 18.04 LTS (Bionic Beaver) 64-Bit Ubuntu Server 20.04 LTS (Focal Fossa) 64-Bit Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-Bit Ubuntu Server 22.04 ARM 64-Bit Ubuntu Server 24.04 LTS (Noble Numbat) 64-Bit Ubuntu Server 26.04 LTS (Resolute Raccoon) 64-Bit Ubuntu Server 26.04 ARM 64-Bit Ubuntu Desktop 10.04 LTS (Lucid Lynx) 32-Bit/64-Bit Ubuntu Desktop 16.04 LTS (Xenial Xerus) 32-Bit/64-Bit CentOS 5.2 32-Bit/64-Bit (wird nur vom Administrationsagenten für Legacy-Linux-Systeme unterstützt, den Sie über die Benutzeroberfläche der Web Console oder von der Kaspersky-Website herunterladen können) CentOS 5.4 32-Bit/64-Bit (wird nur vom Administrationsagenten für Legacy-Linux-Systeme unterstützt, den Sie über die Benutzeroberfläche der Web Console oder von der Kaspersky-Website herunterladen können) CentOS 6.4 32-Bit/64-Bit (wird nur vom Administrationsagenten für Legacy-Linux-Systeme unterstützt, den Sie über die Benutzeroberfläche der Web Console oder von der Kaspersky-Website herunterladen können) CentOS 6.6 32-Bit/64-Bit (wird nur vom Administrationsagenten für Legacy-Linux-Systeme unterstützt, den Sie über die Benutzeroberfläche der Web Console oder von der Kaspersky-Website herunterladen können) CentOS 7.2 und höher 64-Bit CentOS Stream 8 64-Bit CentOS Stream 9 64-Bit CentOS Stream 9 ARM 64-Bit CentOS Stream 10 64-Bit Red Hat Enterprise Linux Server 6.x 32-Bit/64-Bit Red Hat Enterprise Linux Server 7.2 und höher 64-Bit Red Hat Enterprise Linux Server 8.x 64-Bit Red Hat Enterprise Linux Server 9.x 64-Bit Red Hat Enterprise Linux Server 10.x 64-Bit SUSE Linux Enterprise Server 12.5 und höher (alle Service Packs) 64-Bit SUSE Linux Enterprise Server 15 (alle Service Packs) 64-Bit SUSE Linux Enterprise Server 15 (alle Service Packs) ARM 64-Bit openSUSE Leap 15 64-Bit EulerOS 2.0 SP10 64-Bit EulerOS 2.0 SP10 ARM 64-Bit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.4) 32-Bit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.4) 64-Bit (wird nur vom Administrationsagenten für Legacy-Linux-Systeme unterstützt, den Sie über die Benutzeroberfläche der Web Console oder von der Kaspersky-Website herunterladen können) Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.5) 64-Bit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.6) 64-Bit Astra Linux Special Edition RUSB.10015-16 (Release 1) (operatives Update 1.6) 64-Bit Astra Linux Special Edition RUSB.10015-17 (operatives Update 1.7.3) 64-Bit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.7) 64-Bit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.8) 64-Bit Astra Linux Special Edition RUSB.10015-03 (operatives Update 7.6) 64-Bit Astra Linux Special Edition RUSB.10015-37 (operatives Update 7.7) 64-Bit Astra Linux Special Edition RUSB.10152-02 (operatives Update 4.7) ARM 64-Bit Astra Linux Common Edition (operatives Update 2.12) 64-Bit ALT Workstation 11 64-Bit ALT Server 11 64-Bit ALT Education 11 64-Bit ALT Workstation 10.1 64-Bit

ALT Server 10.1 64-Bit
ALT Education 10.1 64-Bit
ALT SP Server 10 32-Bit/64-Bit
ALT SP Server 10 ARM 64-Bit
ALT SP Workstation 10 32-Bit/64-Bit
ALT SP Workstation 10 ARM 64-Bit
ALT 8 SP Server (LKNV.11100-01) 32-Bit/64-Bit
ALT 8 SP Server (LKNV.11100-02) 32-Bit/64-Bit
ALT 8 SP Server (LKNV.11100-03) 32-Bit/64-Bit
ALT 8 SP Workstation (LKNV.11100-01) 32-Bit/64-Bit
ALT 8 SP Workstation (LKNV.11100-02) 32-Bit/64-Bit
ALT 8 SP Workstation (LKNV.11100-03) 32-Bit/64-Bit
Oracle Linux 7 64-Bit
Oracle Linux 8 64-Bit
Oracle Linux 9 64-Bit
Linux Mint 21.1 und höher, 64-Bit
Linux Mint 22.x 64-Bit
AlterOS 7.5 und höher, 64-Bit
AlterOS 2025 64-Bit
GosLinux IC6/7.17 64-Bit
GosLinux IC6/7.2 64-Bit
SberOS 3.4.0 64-Bit
SberOS 3.5.0 64-Bit
SberOS 3.6.1 64-Bit
Plattform V SberLinux OS Server (SLO) 8.10.1 64-Bit
Plattform V SberLinux OS Server (SLO) 9.1 64-Bit
Plattform V SberLinux OS Server (SLO) 9.5.1 64-Bit
Plattform V SberLinux OS Server (SLO) 9.6 64-Bit
Platform V SberLinux OS Server (SLO) 9.7 64-Bit
RED OS 7.3 Server 64-Bit
RED OS 7.3 Certified Edition 64-Bit
RED OS 8 64-Bit
RED OS 8 ARM 64-Bit
ROSA Enterprise Linux Server 7.9 64-Bit
ROSA Enterprise Linux Desktop 7.9 64-Bit
ROSA COBALT 7.9 64-Bit
ROSA CHROME 12 64-Bit
AlmaLinux 8 und höher, 64-Bit
AlmaLinux 9 und höher, 64-Bit
Rocky Linux 8 und höher, 64-Bit
Rocky Linux 9 und höher, 64-Bit
Atlant, Alcyone-Build, Version 2022.02 64-Bit
MSVSPHERE 9.2 SERVER 64-Bit
MSVSPHERE 9.2 ARM 64-Bit
MSVSPHERE 9.4 SERVER 64-Bit
MSVSPHERE 9.4 ARM 64-Bit
SynthesisM Server 8.6 64-Bit
SynthesisM Client 8.6 64-Bit
OSnova 2.* 64-Bit
OSnova 3.* 64-Bit
Kylin 10 64-Bit
EMIAS 1.0 64-Bit
Amazon Linux 2 64-Bit
MosOS 15.5 Arbat 64-Bit
OS MES (Moscow Electronic School) 12 (für Computer und Laptops) 64-Bit
OS MES (Moscow Electronic School) 12 Server 64-Bit

	OS MES (Moscow Electronic School) 12 Server 64-Bit Mostech 64-Bit Mostech Server 64-Bit Fedora Linux Server 41 64-Bit Fedora Linux Workstation 41 64-Bit
Betriebssysteme. macOS	Eine Liste der unterstützten Betriebssysteme finden Sie in der Hilfe zu Kaspersky Endpoint Security for Mac.
Virtualisierungsplattformen	Ausführliche Informationen zu den unterstützten Virtualisierungsplattformen finden Sie in der Online-Hilfe zu Kaspersky Security for Virtualization Light Agent.

Bei Windows-Versionen, die älter als Microsoft Windows Server 2008 R2 (Server-Versionen) und Microsoft Windows 7 (Desktop-Versionen) sind, unterstützt der Administrationsagent die folgenden Funktionen nicht:

- Übertragen von Updates and die Geräte (von Verteilungspunkten verwendet)
- KSN-Proxy (von Verteilungspunkten verwendet)
- Aufgabe zur Untersuchung auf Schwachstellen

Auf Geräten mit Microsoft Windows 10 Version RS4 oder RS5 kann es vorkommen, dass Kaspersky Security Center nicht in der Lage ist, Schwachstellen zu finden, wenn diese sich in Ordnern mit aktivierter Unterscheidung zwischen Groß- und Kleinschreibung befinden.

Stellen Sie vor der Installation des Administrationsagenten auf Geräten mit Windows 7, Windows Server 2008, Windows Server 2008 R2 oder Windows MultiPoint Server 2011 sicher, dass Sie das Sicherheitsupdate KB3063858 für Windows-Betriebssysteme installiert haben (Sicherheitsupdate für Windows 7 (KB3063858), Sicherheitsupdate für Windows 7 für Systeme auf x64-Basis (KB3063858), Sicherheitsupdate für Windows Server 2008 (KB3063858), Sicherheitsupdate für Windows Server 2008 x64 Edition (KB3063858), Sicherheitsupdate für Windows Server 2008 R2 x64 Edition (KB3063858).

Unter Windows XP führt der Administrationsagent einige Vorgänge möglicherweise nicht korrekt aus.

Sie können den Administrationsagenten für Windows XP nur unter Microsoft Windows XP installieren oder aktualisieren. Die unterstützten Editionen von Microsoft Windows XP und die entsprechenden Versionen des Administrationsagenten sind in der Liste mit unterstützten Betriebssystemen aufgeführt. Sie können die erforderliche Version des Administrationsagenten für Microsoft Windows XP von dieser Seite herunterladen.

Es wird empfohlen, den Administrationsagenten für Linux mit der gleichen Version wie Kaspersky Security Center Linux zu installieren.

Kaspersky Security Center Linux bietet vollständige Unterstützung für die Administrationsagenten derselben oder neuerer Versionen.

Der Administrationsagent für macOS wird zusammen mit der Kaspersky-Sicherheitsanwendung für dieses Betriebssystem bereitgestellt.

Kompatible Anwendungen und Lösungen von Kaspersky

Kaspersky Security Center Linux unterstützt die zentralisierte Bereitstellung und Verwaltung aller derzeit unterstützten Kaspersky-Anwendungen und -Lösungen. Weitere Informationen über die Versionen der Anwendungen und Lösungen finden Sie auf der Webseite mit dem Lebenszyklus der Anwendung.

Unterstützte Kaspersky-Anwendungen:

- Kaspersky Endpoint Security für Windows (Unterstützung für Dateiserver)
- Kaspersky Endpoint Security für Linux (Unterstützung für Dateiserver)
- Kaspersky Endpoint Security für Linux Elbrus Edition
- Kaspersky Endpoint Security for Mac
- Kaspersky Endpoint Security für Android
- Kaspersky Endpoint Security for Aurora
- Kaspersky Security für iOS
- Kaspersky Industrial CyberSecurity for Linux Nodes
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks
- Kaspersky Endpoint Agent
- Kaspersky Embedded Systems Security für Windows
- Kaspersky Embedded Systems Security für Linux
- Kaspersky Security for Virtualization Light Agent
- KATA Sandbox (eine der Komponenten der Kaspersky Anti Targeted Attack Platform)
- Kaspersky Thin Client
- Kaspersky NGFW
- Kaspersky Sandbox
- Kaspersky Vulnerability Management

Kaspersky Security Center Linux ist in den folgenden Lösungen enthalten:

- Kaspersky Endpoint Detection and Response Optimum
- Kaspersky Managed Detection and Response
- Kaspersky Next XDR Optimum

Informationen über die Anwendungsversionen finden Sie auf der Webseite des Produkt-Supports mit dem Lebenszyklus.

Bekannte Probleme

Single Sign-On (SSO) wird für Kaspersky Industrial CyberSecurity for Networks nicht unterstützt.

Über die Kompatibilität der Kaspersky Security Center Linux-Komponenten

Die folgende Tabelle enthält Informationen zur Kompatibilität der Komponenten von Kaspersky Security Center Linux.

Kompatibilität der Komponenten von Kaspersky Security Center Linux

Komponente	Kompatibel mit
Kaspersky Security Center 16.3 Linux Administrationsserver	• Kaspersky Security Center Web Console der folgenden Versionen: 16.3, 16.2, 16.1 • Kaspersky Security Center Administrationsagent der folgenden Versionen: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15
Kaspersky Security Center 16.3 Web Console	Kaspersky Security Center Linux Administrationsserver der folgenden Versionen: 16.3, 16.2, 16.1, 16
Kaspersky Security Center 16.3 Linux Primärer Administrationsserver	Sekundäre Administrationsserver: • Kaspersky Security Center Linux der folgenden Versionen: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15 • Kaspersky Security Center Windows der folgenden Versionen 15.1
Kaspersky Security Center 16.3 Linux Sekundärer Administrationsserver	Primäre Administrationsserver: • Kaspersky Security Center Linux der folgenden Versionen: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15 • Kaspersky Security Center Windows der folgenden Versionen 15.1

Komponente	Kompatibel mit
Kaspersky Security Center 16.3 Administrationsagent	Administrationsserver: • Kaspersky Security Center Linux der folgenden Versionen: 16.3, 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15 • Kaspersky Security Center Windows der folgenden Versionen 15.1
Backup und Wiederherstellung der Daten des Kaspersky Security Center Administrationsserver	Die Backup und Wiederherstellung wird ab den folgenden Versionen des Kaspersky Security Center Linux Administrationsservers unterstützt: 16.2, 16.1, 16, 15.4, 15.3, 15.2, 15.1, 15

Es wird empfohlen, sowohl den Kaspersky Security Center Administrationsserver als auch die Kaspersky Security Center Web Console in der jeweils aktuellsten Version zu verwenden. Andernfalls wird die Funktionalität von Kaspersky Security Center möglicherweise eingeschränkt. Sie können den Kaspersky Security Center Administrationsserver und die Kaspersky Security Center Web Console unabhängig voneinander installieren und aktualisieren. In diesem Fall müssen Sie sicherstellen, dass die Version der installierten Kaspersky Security Center Web Console mit der Version des Administrationsservers, mit dem Sie eine Verbindung herstellen, kompatibel ist:

Wenn Sie über die neueste Version von Kaspersky Security Center Web Console und eine frühere Version von Kaspersky Security Center verwenden und während der Domänenauthentifizierung ein Fehler auftritt, enthält der Fehlertext eine Standardmeldung.

Der Kaspersky Security Center 16.3 Linux Administrationsserver ist auch mit dem Kaspersky Security Center 16.3 Administrationsagenten der folgenden Versionen kompatibel:

- 10.5.1781

  Diese Version unterstützt Microsoft Windows XP Professional mit Service Pack 2. Sie können diese Version des Administrationsagenten über den Technischen Support anfordern.

- 14.0.0.20023

  Diese Version unterstützt Microsoft Windows XP Professional mit Service Pack 3. Sie können diese Version des Administrationsagenten von dieser Seite herunterladen.

Ausführliche Informationen dazu finden Sie in der Liste der unterstützten Betriebssysteme.

Vergleich von Kaspersky Security Center: Windows-basiert vs. Linux-basiert

Kaspersky bietet Kaspersky Security Center als lokale Lösung für zwei Plattformen – Windows und Linux. Bei der Windows-basierten Lösung installieren Sie den Administrationsserver auf einem Windows-Gerät und bei der Linux-basierten Lösung ist die Administrationsserver-Version für die Installation auf einem Linux-Gerät vorgesehen. Diese Online-Hilfe enthält Informationen zu Kaspersky Security Center. Ausführliche Informationen zur Windows-basierten Lösung finden Sie in der Online-Hilfe von Kaspersky Security Center Windows.

Die folgende Tabelle bietet einen Vergleich der Hauptfunktionen von Kaspersky Security Center als Windows-basierte Lösung und als Linux-basierte Lösung.

Funktion oder Eigenschaft	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.2 Linux
Administrationsserver		
Standort des Datenbankmanagementsystems (DBMS)	On-premises	On-premises (Microsoft SQL wird nicht unterstützt)
Betriebssystem, auf dem der Administrationsserver installiert werden soll	Windows	Linux
Hierarchie des Administrationsservers	✓	✓
Unterstützung für virtuelle Administrationsserver	✓	✓
Kaspersky Security Center Failover-Cluster bereitstellen	✓ Nur ein Single-Site-Cluster	✓ Ab Kaspersky Security Center 16.2 Linux werden geografisch verteilte Failover-Cluster unterstützt.
Verwenden von SNMP, um Statistiken des Administrationsservers an Anwendungen von Drittanbietern zu senden	✓	✓
Webserver zum Veröffentlichen von Installationspaketen und anderen Dateien	✓	✓
Verwaltungskonsole		
Typ der Verwaltungskonsole	MMC-basiert und webbasiert	Webbasiert
Betriebssystem, auf dem die webbasierte Verwaltungskonsole installiert werden soll	Windows oder Linux	Linux
Anmelden an der Konsole mit Domänenauthentifizierung	✓	✓
Verwaltung von Client-Geräten und Administrationsgruppen		
Maximale Anzahl verwalteter Geräte (pro Administrationsserver)	100.000 (mit Microsoft SQL Server)	50.000 (mit PostgreSQL und Postgres Pro)
Netzwerkabfrage	✓	✓
Schutz von verwalteten Windows-, macOS- und Linux-verwalteten Geräten	✓	✓
Schutz von mobilen Geräten	✓ Grundlegende Verwaltung mobiler Geräte	✓ MDM und Verwendung der Funktionen von Kaspersky Secure Mobility Management (unter Lizenz)
Verwaltung des Schutzes von virtuellen Maschinen	✓	✓
Schutz der Public-Cloud-Infrastruktur	✓	—
Remote-Desktopverbindung mit einem Client-Gerät	✓	✓
Verschlüsselung und Datenschutz	✓ Auf Windows-basierten verwalteten Geräten mit installiertem Kaspersky Endpoint Security für Windows oder Kaspersky Endpoint Security for Mac	✓ Auf Windows-basierten verwalteten Geräten mit installiertem Kaspersky Endpoint Security für Windows oder Kaspersky Endpoint Security for Mac
Unterstützung von Clustern und Server-Arrays in Administrationsgruppen	✓	✓
Hierarchie der Administrationsgruppen	✓	✓
Hinzufügen eines Verbindungs-Gateways als Verteilungspunkt innerhalb der DMZ	✓ (wird von der Web Console nicht unterstützt)	✓
Benutzerverwaltung		

Funktion oder Eigenschaft	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.2 Linux
Erstellen und Verwalten von Benutzerkonten	✓	✓
Verwaltung von Kaspersky-Anwendungen		
Anwendungsrichtlinien	✓	✓
Aufgaben für Kaspersky-Anwendungen	✓	✓
Kaspersky Security Network	✓	✓
KSN-Proxy	✓	✓
Kaspersky Private Security Network	✓	✓
Zentralisierte Bereitstellung von Lizenzschlüsseln für Kaspersky-Anwendungen	✓	✓
Ferndiagnose der Client-Geräte	✓	✓
Automatisches Aktualisieren der Kaspersky-Anwendungen	✓	✓
Unterstützung der Adaptiven Kontrolle von Anomalien	✓	✓
Gerätezentrierte Sicherheitsverwaltung	✓	✓
Benutzerzentrierte Sicherheitsverwaltung	✓	✓
Systemverwaltung		
Bereitstellen von Betriebssystemen auf Client-Geräten	✓	—
Verwalten der Lizenzen von Drittanbietern	✓	Wird im Jahr 2026 implementiert
Administrationsserver als WSUS-Server verwenden	✓	✓ (Nur im passivem Modus für die Suche nach Windows-Updates)
Verwalten von Programmen von Drittanbietern auf Client-Geräten		
Installieren von Updates für Drittanbieter-Programme und Beheben von Schwachstellen in Drittanbieter-Programmen	✓	✓
Programmkategorien importieren und exportieren	✓ (wird von der Web Console nicht unterstützt)	Wird im Jahr 2026 implementiert
Überwachung, Berichterstattung und Audit		
Umgang mit Objekt-Revisionen	✓	✓
Vergleichen von Richtlinienrevisionen	✓	✓
Anzeigen und Bearbeiten der Alarme, die von Kaspersky Endpoint Detection and Response Optimum erkannt wurden	✓	✓
Benachrichtigungen über Ereignisse, die auf verwalteten Geräten auftreten	✓	✓
Überwachung des Richtlinienstatus und Aufgabenstatus	✓	✓
Integrationen		
Integration mit Kaspersky Managed Detection and Response	✓	✓

Funktion oder Eigenschaft	Kaspersky Security Center 15.1 Windows	Kaspersky Security Center 16.2 Linux
Integration von SIEM-Systemen	✓	✓
Aggregation von Alarmen und Ausführen von Reaktionsmaßnahmen über Active Directory, KASAP und Kaspersky TIP Sandbox	–	✓ Sie müssen den Administrationsserver unter einer Lizenz für Kaspersky Next XDR Optimum aktivieren und anschließend den Lizenzschlüssel von Kaspersky Next XDR Optimum für Ihre verwalteten Anwendungen bereitstellen.

Über die Kaspersky Security Center Cloud Console

Die Verwendung von Kaspersky Security Center als lokal installierte Anwendung (on-premises) bedeutet, dass Sie Kaspersky Security Center zusammen mit dem Administrationsserver auf einem lokalen Gerät installieren, und die Netzwerksicherheit entweder über die auf der Microsoft Management Console basierenden Verwaltungskonsole (nur für Kaspersky Security Center Windows verfügbar) oder über die Kaspersky Security Center Web Console verwalten.

Alternativ dazu können Sie Kaspersky Security Center auch als Cloud-Dienst verwenden. In diesem Fall wird für Sie Kaspersky Security Center von Kaspersky-Experten in einer Cloud-Umgebung installiert und verwaltet, und Kaspersky gewährt Ihnen den Zugriff auf den Administrationsserver in Form eines Dienstes. Sie verwalten die Netzwerksicherheit durch eine cloudbasierte Verwaltungskonsole namens Kaspersky Security Center Cloud Console. Die Benutzeroberfläche dieser Konsole ist ähnlich der von Kaspersky Security Center Web Console.

Die Benutzeroberfläche und Dokumentation von Kaspersky Security Center Cloud Console sind in folgenden Sprachen verfügbar:

- Englisch
- Französisch
- Deutsch
- Italienisch
- Japanisch
- Portugiesisch (Brasilien)
- Russisch
- Vereinfachtes Chinesisch
- Spanisch
- Spanisch (LATAM)
- Traditionelles Chinesisch

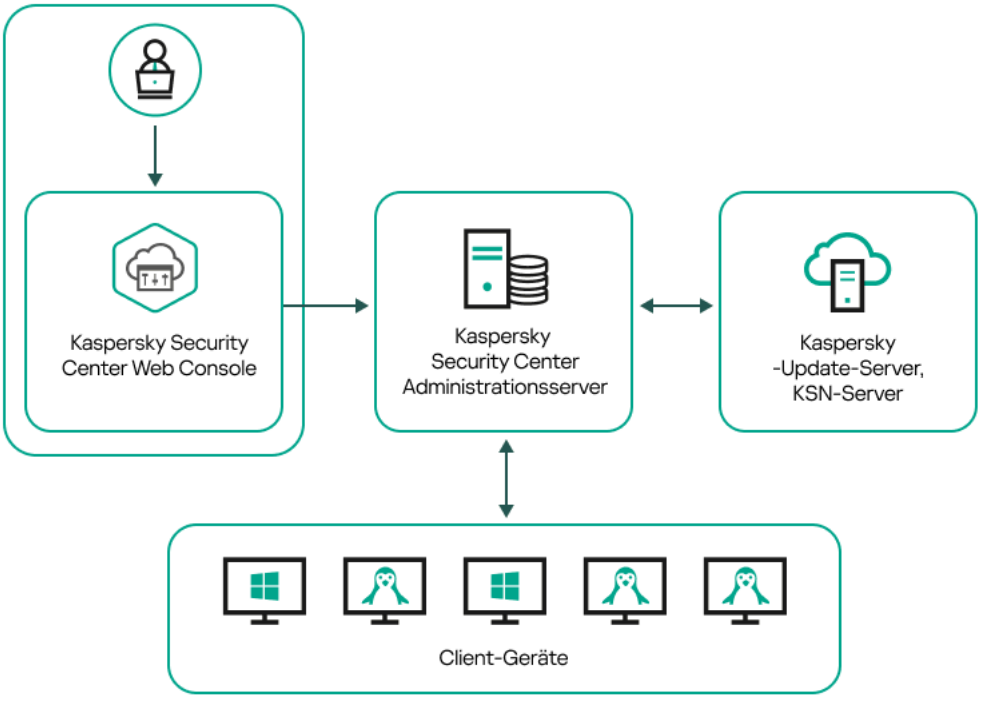
Weitere Informationen zu Kaspersky Security Center Cloud Console und seinen Funktionen finden Sie in der Dokumentation von Kaspersky Security Center Cloud Console und in der Dokumentation von Kaspersky Endpoint Security for Business.

Architektur und grundlegende Konzepte

In diesem Abschnitt werden die Programmarchitektur und die grundlegenden Konzepte von Kaspersky Security Center Linux erläutert.

Architektur

Dieser Abschnitt enthält eine Beschreibung der Komponenten von Kaspersky Security Center und deren Interaktion.



Architektur von Kaspersky Security Center Linux

Kaspersky Security Center Linux umfasst die folgenden Hauptkomponenten:

- **Kaspersky Security Center Web Console**. Bietet eine Weboberfläche zum Erstellen und Verwalten des Schutzsystems in dem von Kaspersky Security Center verwalteten Netzwerk des Kundenunternehmens.
- **Kaspersky Security Center Administrationsserver** (auch als *Server* bezeichnet). Führt die Funktionen zum zentralen Speichern von Daten über die im Firmennetzwerk installierten Anwendungen und deren Verwaltung aus.
- **Kaspersky-Update-Server**. HTTP(S)-Server bei Kaspersky, von denen Kaspersky-Anwendungen Updates für Datenbanken und Anwendungsmodule beziehen.
- **KSN-Server**. Server, die eine Datenbank von Kaspersky mit ständig aktualisierten Informationen über die Reputation von Dateien, Web-Ressourcen und Software umfassen. Kaspersky Security Network gewährleistet eine schnellere Reaktion der Kaspersky-Anwendungen auf Bedrohungen, erhöht die Leistungsfähigkeit der Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.
- **Client-Geräte.** Von Kaspersky Security Center Linux geschützte Geräte eines Kundenunternehmens. Auf jedem zu schützenden Gerät muss eine der Sicherheitsanwendungen von Kaspersky installiert sein.

Diagramm der Softwareverteilung für Kaspersky Security Center Linux Administrationsserver und Kaspersky Security Center Web Console

Die nachfolgende Abbildung zeigt das Diagramm der Bereitstellung für Kaspersky Security Center Linux Administrationsserver Linux und Kaspersky Security Center Web Console.

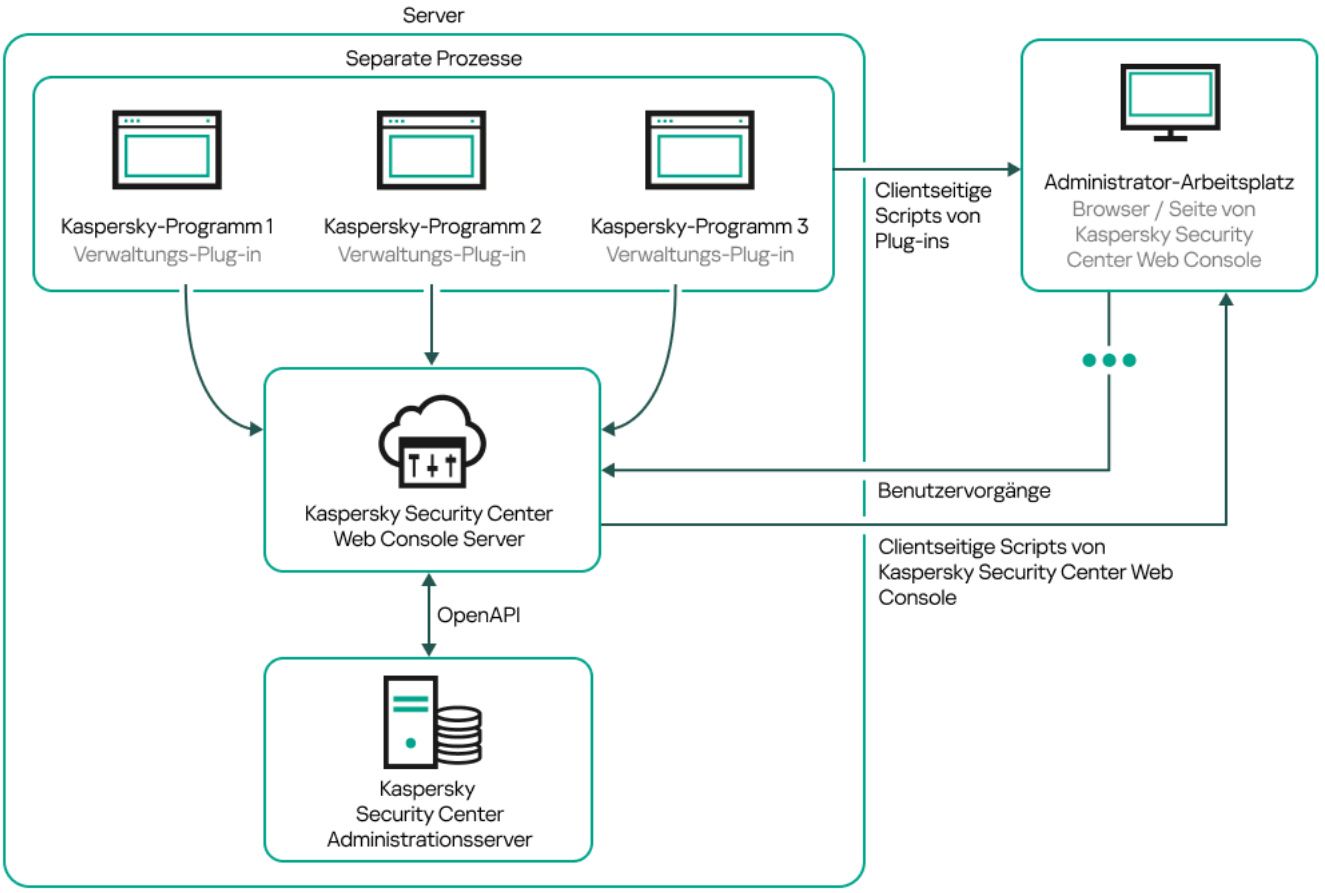


Diagramm der Softwareverteilung für Kaspersky Security Center Linux Administrationsserver und Kaspersky Security Center Web Console

Verwaltungs-Plug-ins für Anwendungen von Kaspersky, die auf geschützten Geräten installiert sind (ein Plug-in für jede Anwendung) werden gemeinsam mit dem Server der Web Console von Kaspersky Security Center verteilt.

Als Administrator greifen Sie mittels eines Browsers auf Ihrer Arbeitsstation auf Kaspersky Security Center Web Console zu.

Wenn Sie bestimmte Aktionen in Kaspersky Security Center Web Console durchführen kommuniziert der Server der Web Console von Kaspersky Security Center mit dem Kaspersky Security Center Linux Administrationsserver über OpenAPI. Der Server der Web Console von Kaspersky Security Center fordert die gewünschten Informationen vom Kaspersky Security Center Linux Administrationsserver an und zeigt die Ergebnisse Ihrer Vorgänge in Kaspersky Security Center Web Console an.

Ports, die von Kaspersky Security Center Linux verwendet werden

Die folgenden Tabellen listen die vom Administrationsserver und von den Client-Geräten verwendeten Standardports auf. Bei Bedarf können Sie jede dieser standardmäßigen Portnummern ändern.

Ports, die von Kaspersky Security Center Linux Administrationsserver verwendet werden

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
8060	klcsweb	TCP	Weitergabe der veröffentlichten Installationspakete an Client-Geräte	Installationspakete veröffentlichen. Die standardmäßige Portnummer können Sie im Abschnitt **Webserver** im Eigenschaftenfenster des Administrationsservers ändern. Dieser Port ist optional. Aus Sicherheitsgründen wird die Verwendung des TCP-Ports 8061 empfohlen.
8061	klcsweb	TCP (TLS)	Weitergabe der veröffentlichten Installationspakete an Client-Geräte	Installationspakete veröffentlichen. Die standardmäßige Portnummer können Sie im Abschnitt **Webserver** im Eigenschaftenfenster des Administrationsservers ändern.
13000	klserver	TCP (TLS)	Aufnahme der Verbindungen von Administrationsagenten und sekundären Administrationsservern; wird auch auf den sekundären Servern für die Aufnahme der Verbindungen vom primären Administrationsserver verwendet (beispielsweise wenn sich der sekundäre Server in einer DMZ befindet)	Verwaltung von Client-Geräten und sekundären Administrationsservern. Sie können die Nummer des standardmäßigen Ports für den Empfang von Verbindungen von Administrationsagenten ändern, wenn Sie während der Installation von Kaspersky Security Center Linux die Verbindungsports konfigurieren. Sie können die Nummer des standardmäßigen Ports für den Empfang von Verbindungen von sekundären Administrationsservern ändern, wenn Sie eine Hierarchie von Administrationsservern erstellen.
13000	klserver	UDP	Annahme der Informationen von Administrationsagenten über das Deaktivieren von Geräten	Verwaltung der Client-Geräte. Sie können die standardmäßige Portnummer in den Richtlinieneinstellungen des Administrationsagenten ändern.
13291	klserver	TCP (TLS)	Verwenden des klakaut-Tools zur Ausführungsautomatisierung der Vorgänge von Kaspersky Security Center Linux	Arbeiten mit dem klakaut-Tool. Das Tool "klakaut" und das entsprechende Hilfesystem befinden sich im Installationsordner von Kaspersky Security Center Linux. Dieser Port ist standardmäßig geschlossen. Wenn Sie das Tool "klakaut" verwenden möchten, um die Vorgänge von Kaspersky Security Center Linux zu automatisieren, öffnen Sie den Port 13291 anhand des Tools "klscflag".
13299	klserver	TCP (TLS)	Verbindungen von der Identitäts- und Zugriffsverwaltung (IAM) zum Administrationsserver annehmen; Verbindungen zum Administrationsserver über OpenAPI annehmen	Verwalten des Administrationsservers mittels Kaspersky Security Center Web Console und arbeiten mit OpenAPI. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern (im Unterabschnitt **Verbindungsports** des Abschnitts **Allgemein**) oder, wenn Sie eine Hierarchie von Administrationsservern erstellen.

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
14000	klserver	TCP	Annahme der Verbindungen von den Administrationsagenten	Verwaltung der Client-Geräte. Sie können die standardmäßige Portnummer ändern, wenn Sie während der Installation von Kaspersky Security Center Linux die Verbindungsports konfigurieren oder wenn Sie ein Client-Gerät manuell mit dem Administrationsserver verbinden. Dieser Port ist optional und standardmäßig geschlossen. Aus Sicherheitsgründen wird die Verwendung des TCP-Ports 13000 empfohlen.
13111 (nur, wenn der KSN-Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	TCP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern.
15111 (nur, wenn der KSN-Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	UDP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern.
17111 (nur, wenn der KSN-Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	HTTPS	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern.
17000	klactprx	TCP (TLS)	Annahme der Verbindungen zur Anwendungsaktivierung auf verwalteten Geräten	Proxyserver zur Aktivierung von verwalteten Geräten. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers ändern (im Unterabschnitt **Zusätzliche Ports** des Abschnitts **Allgemein**).
13292 (nur wenn Sie mobile Geräte verwalten)	klserver	TCP (TLS)	Annahme der Verbindungen von mobilen Geräten	Verwaltung mobiler Geräte. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Administrationsservers in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console ändern.
19170	klserver	HTTPS (TLS)	Tunneln der Verbindungen mit verwalteten Geräten mittels des Tools "klsctunnel"	Remote-Verbindungen mit verwalteten Geräten herstellen mittels Kaspersky Security Center Web Console. Sie können die Standard-Portnummer im Eigenschaftsfenster des Administrationsservers ändern (**Allgemein** → **Verbindungsports** → **RDP-Verbindung tunneln**).
4444	kliam	HTTPS	Authentifizierung mithilfe des OpenID Connect-Protokolls	Austausch von Authentifizierungstoken zwischen dem Browser und der Identitäts- und Zugriffsverwaltung (IAM).
9050	kliam	HTTPS	Verbindung zum Administrationsserver mithilfe von IAM	Austausch von Authentifizierungstoken zwischen Kaspersky Security Center Web Console und IAM

Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät, auf dem sich die Datenbank befindet, bereitstellen (zum Beispiel: Port 3306 für MariaDB). Relevante Informationen finden Sie in der DBMS-Dokumentation.

Die folgende Tabelle zeigt den Port, der vom iOS™ MDM-Server verwendet wird (Nur bei Verwaltung mobiler Geräte).

Port, der vom iOS MDM-Server verwendet wird

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
443	kliosmdmservicesrv	TCP (TLS)	Empfangen von Verbindungen von mobilen iOS-Geräten	Verwaltung mobiler Geräte. Sie können die standardmäßige Portnummer ändern, wenn Sie den iOS MDM-Server installieren.

Die folgende Tabelle zeigt den vom Server der Kaspersky Security Center Web Console verwendeten Port. Es kann sich dabei sowohl um dasselbe Gerät handeln, auf dem der Administrationsserver installiert ist, als auch um ein anderes Gerät.

Port, der vom Server der Web Console von Kaspersky Security Center verwendet wird

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
8080	Node.js: Serverseitiges JavaScript	TCP (TLS)	Empfangen von Verbindungen vom Webbrowser zur Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Sie können die standardmäßige Portnummer ändern, wenn Sie Kaspersky Security Center Web Console installieren. Wenn Sie die Kaspersky Security Center Web Console auf dem ALT Linux-Betriebssystem installieren, müssen Sie eine andere Portnummer als 8080 angeben, da Port 8080 von dem Betriebssystem verwendet wird.

Die folgende Tabelle listet die Ports auf, die von verwalteten Geräten mit installiertem Administrationsagenten verwendet werden.

Ports, die vom Administrationsagenten verwendet werden

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
15000	klnagent	UDP	Verwaltungssignale vom Administrationsserver oder Verwaltungspunkt an die Administrationsagenten	Verwaltung der Client-Geräte. Sie können die standardmäßige Portnummer in den Richtlinieneinstellungen des Administrationsagenten ändern.
15000	klnagent	UDP-Broadcast	Abrufen von Daten über andere Administrationsagenten in derselben Broadcast-Domäne (die Daten werden dann an den Administrationsserver gesendet)	Zustellung von Updates und Installationspaketen.
15001	klnagent	UDP	Empfangen von Multicast-Anfragen von einem Verteilungspunkt (falls verwendet)	Empfang von Updates und Installationspaketen von einem Verteilungspunkt. Sie können die standardmäßige Portnummer im Eigenschaftenfenster des Verteilungspunkts ändern.
30522, 30523 (Ports der localhost-Schnittstelle)	klnagent	TCP	Abrufen der Anwendungsupdates von Kaspersky für den Administrationsserver über die FileTransferBridge-Komponente	Verwaltete Geräte, die Updates für Kaspersky-Anwendungen von einem Administrationsserver abrufen, der als Quelle für das Datenbank-Update angegeben ist.

Bitte beachten Sie, dass der Prozess "klnagent" auch freie Ports aus dem dynamischen Portbereich eines Endpoint-Betriebssystems anfordern kann. Diese Ports werden dem klnagent-Prozess automatisch vom Betriebssystem zugewiesen, was dazu führen kann, dass der klnagent-Prozess einige Ports verwendet, die von einer anderen Software verwendet werden. Wenn der klnagent-Prozess die Ausführung der Software beeinträchtigt, ändern Sie die Porteinstellungen in dieser Software. Alternativ können Sie den standardmäßigen dynamischen Portbereich in Ihrem Betriebssystem ändern, um den Port auszuschließen, der von der betroffenen Software verwendet wird.

Beachten Sie auch, dass die Empfehlungen zur Kompatibilität von Kaspersky Security Center Linux mit Drittanbieter-Programmen nur referenziellen Charakter besitzen und möglicherweise nicht auf neuere Versionen der Drittanbieter-Programme zutreffen. Die beschriebenen Empfehlungen zur Port-Konfiguration basieren auf den Erfahrungen des Technischen Supports und unseren bewährten Verfahren.

Die nachfolgende Tabelle listet die Ports auf, die von einem verwalteten Gerät mit installiertem Administrationsagenten, welcher als Verteilungspunkt fungiert, verwendet werden. Die aufgelisteten Ports werden von den Verteilungspunkt-Geräten zusätzlich zu den Ports verwendet, die von Administrationsagenten verwendetet werden (siehe Tabelle oben).

Ports, die von einem Administrationsagenten verwendet werden, der als Verteilungspunkt fungiert

Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports	Gültigkeitsbereich
13000	klnagent	TCP (TLS)	Verbindungen von Administrationsagenten und Verbindungs-Gateways empfangen	Verwaltung von Client-Geräten, Zustellung von Updates und Installationspaketen. Sie können die standardmäßige Portnummer in den Eigenschaften des Verteilungspunkts ändern.
13111 (nur, wenn der KSN-Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	TCP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer in den Eigenschaften des Verteilungspunkts ändern.
15111 (nur, wenn der KSN-Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	UDP	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer in den Eigenschaften des Verteilungspunkts ändern.
17111 (nur, wenn der KSN-Proxy-Service auf dem Gerät ausgeführt wird)	ksnproxy	HTTPS	Annahme der Anfragen von verwalteten Geräten an den KSN-Proxyserver	KSN-Proxyserver. Sie können die standardmäßige Portnummer in den Eigenschaften des Verteilungspunkts ändern.
13295 (nur wenn Sie den Verteilungspunkt als Push-Server verwenden)	klnagent	TCP (TLS)	Annehmen der Verbindungen von Client-Geräten	Push-Server. Sie können die standardmäßige Portnummer in den Eigenschaften des Verteilungspunkts ändern.
8060	klcsweb	TCP	Weitergabe der veröffentlichten Installationspakete an Client-Geräte	Installationspakete veröffentlichen. Sie können die standardmäßige Portnummer im Abschnitt **Webserver** im Eigenschaftsfenster des Administrationsservers ändern.
8061	klcsweb	TCP (TLS)	Weitergabe der veröffentlichten Installationspakete an Client-Geräte	Installationspakete veröffentlichen. Sie können die standardmäßige Portnummer im Abschnitt **Webserver** im Eigenschaftsfenster des Administrationsservers ändern.

Die folgende Tabelle listet die Ports auf, die vom Gerät eines Domänencontrollers verwendet werden.

Ports, die das Gerät eines Domänencontrollers verwendetet

Portnummer	Protokoll	Zweck des Ports	Gültigkeitsbereich
389	LDAP über TCP oder UDP	Verbindung zu einem LDAP-Server herstellen	Abfrage des Domänencontrollers
636	LDAP über TLS	Verbindung zu einem LDAP-Server herstellen	Abfrage des Domänencontrollers

Die folgende Tabelle enthält den Port, der auf Client-Geräten mit installiertem Administrationsagenten geöffnet sein muss.

Verwendeter Port auf einem nicht zugeordneten Client-Gerät

Portnummer	Protokoll	Zweck des Ports	Gültigkeitsbereich
22	SSH	SSH-Verbindung zu einem Client-Gerät	Remote-Installation von Kaspersky-Anwendungen

Von Kaspersky Security Center Web Console verwendete Ports

Die untenstehende Tabelle listet alle Ports auf, die auf dem Gerät geöffnet werden müssen, auf dem der Server der Web Console von Kaspersky Security Center (auch Kaspersky Security Center Web Console genannt) installiert ist.

Von Kaspersky Security Center Web Console verwendete Ports

Portnummer	Name des Dienstes	Protokoll	Zweck des Ports	Gültigkeitsbereich
2001	Kaspersky Security Center Server für Produkt-Plug-ins	HTTPS	API-Port, der von den Prozessen des Verwaltungs-Plug-ins verwendet wird, um Anfragen vom "Kaspersky Security Center Web Console Management Service" zu empfangen.	Ausführen von Knoten-Prozessen der Verwaltungs-Plug-ins
1329, 2003	Verwaltungsdienst der Kaspersky Security Center Web Console	HTTPS	API-Ports, die verwendet werden, um Anfragen vom "Kaspersky Security Center Web Console Management Service" desselben Geräts zu empfangen.	Aktualisierung der Komponenten von Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	API-Port, der verwendet wird, um Anfragen vom "Kaspersky Security Center Web Console Management Service" desselben Geräts zu empfangen.	Ausführen von Knoten-Prozessen von Kaspersky Security Center Web Console
8200	—	HTTP	API-Port, der für die Erstellung von Zertifikaten unter Verwendung von HashiCorp Vault verwendet wird (Weitere Informationen entnehmen Sie der Website von HashiCorp Vault).	Installieren von Kaspersky Security Center Web Console und Aktualisieren der Komponenten von Kaspersky Security Center Web Console
4222	Kaspersky Security Center Web Console NATS	HTTPS	API-Ports des NATS-basierten Message Brokers, der für die Kommunikation zwischen den Prozessen von Kaspersky Security Center Web Console und den Verwaltungs-Plug-ins verwendet werden Der Port 8222 wird zur NATS-Überwachung verwendet.	Interaktionen zwischen Kaspersky Security Center Web Console und Verwaltungs-Plug-ins
4444	Identitäts- und Zugriffsverwaltung (IAM)	HTTPS	Port, der vom OpenID Connect-Authentifizierungsprotokoll verwendet wird.	Austausch von Authentifizierungstoken zwischen Kaspersky Security Center Web Console und der Identitäts- und Zugriffsverwaltung (IAM)
9050	IAM	HTTPS	Port, der von der IAM verwendet wird.	Interaktionen zwischen Kaspersky Security Center Web Console und der IAM

Grundbegriffe

In diesem Abschnitt werden die Grundbegriffe von Kaspersky Security Center Linux erläutert.

Administrationsserver

Die Komponenten von Kaspersky Security Center ermöglichen eine Remote-Programmverwaltung der auf Client-Geräten installierten Kaspersky-Anwendungen.

Geräte, auf welchen die Komponente "Administrationsserver" installiert ist, werden als *Administrationsserver* bezeichnet (im Weiteren auch *Server* genannt). Administrationsserver müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Der Administrationsserver wird auf dem Gerät als Dienst mit den folgenden Attributen installiert:

- Unter dem Namen `kladminserver_srv`
- Mit automatischem Start bei Start des Betriebssystems
- Unter dem Benutzerkonto `ksc` oder unter dem Benutzerkonto, das bei Installation des Administrationsservers ausgewählt wurde

Eine vollständige Liste der Installationseinstellungen finden Sie in folgendem Artikel: Kaspersky Security Center Linux installieren.

Der Administrationsserver führt folgende Funktionen aus:

- Speicherung der Struktur der Administrationsgruppen
- Speicherung von Informationen über die Konfiguration der Client-Geräte
- Organisation der Datenverwaltung für Anwendungspakete
- Remote-Installation von Anwendungen auf Client-Geräten und Löschen von Anwendungen
- Datenbanken-Update und Update der Module von Kaspersky-Anwendungen
- Verwaltung von Richtlinien und Aufgaben auf Client-Geräten
- Speicherung von Informationen über die auf den Client-Geräten aufgetretenen Ereignisse
- Erstellen von Berichten über die Ausführung von Kaspersky-Anwendungen
- Verteilung von Lizenzschlüsseln auf Client-Geräte, sowie Speicherung von Informationen über die Lizenzschlüssel
- Senden von Benachrichtigungen über den Status der Aufgabenausführung (z. B. über einen Virenfund auf einem Client-Gerät)

Namensgebung für Administrationsserver in der Anwendungsoberfläche

Auf der Benutzeroberfläche von Kaspersky Security Center Web Console können Administrationsserver die folgenden Namen haben:

- Name des Geräts mit dem Administrationsserver, z. B. "*Gerätename*" oder "Administrationsserver: *Gerätename*".
- IP-Adresse des Geräts mit dem Administrationsserver, z. B. "*IP-Adresse*" oder "Administrationsserver: *IP-Adresse*".

- Sekundäre Administrationsserver und virtuelle Administrationsserver haben benutzerdefinierte Namen, die Sie beim Verbinden eines virtuellen oder sekundären Administrationsservers mit dem primären Administrationsserver angeben.

- Wenn Sie Kaspersky Security Center Web Console auf einem Linux-Gerät installiert haben und verwenden, zeigt die Anwendung die Namen von Administrationsservern, die Sie als "vertrauenswürdig" eingestuft haben, in einer Antwort-Datei an.

Sie können über Kaspersky Security Center Web Console eine Verbindung zum Administrationsserver herstellen.

Hierarchie des Administrationsservers

Administrationsserver können eine Hierarchie bilden. Jeder Administrationsserver kann über mehrere sekundäre Administrationsserver (im Folgenden auch *sekundäre Server*) auf verschiedenen Hierarchieebenen verfügen. Die Verschachtelungstiefe der sekundären Server ist nicht beschränkt. Zu den Administrationsgruppen des primären Administrationsservers gehören die Client-Geräte aller sekundärer Administrationsserver. So können unabhängige Bereiche des Computernetzwerks durch verschiedene Administrationsserver verwaltet werden, die wiederum durch einen primären Server administriert werden.

In einer Hierarchie kann ein Linux-basierter Administrationsserver sowohl als primärer Server als auch als sekundärer Server fungieren. Der primäre Linux-basierte Server kann sowohl Linux-basierte als auch Windows-basierte sekundäre Server verwalten. Ein primärer Server auf Windows-Basis kann einen sekundären Server auf Linux-Basis verwalten.

Ein *virtueller Administrationsserver* stellt einen besonderen Fall eines sekundären Administrationsservers dar.

Die Hierarchie der Administrationsserver lässt sich zu folgenden Zwecken verwenden:

- Beschränkung der Belastung des Administrationsservers (im Vergleich zu einem einzigen im Netzwerk installierten Server).

- Verringerung des Datenverkehrs im Netzwerk und Vereinfachung der Arbeit mit Remote-Niederlassungen. Sie müssen keine Verbindungen zwischen dem primären Administrationsserver und allen Geräten im Netzwerk herstellen, die sich zum Beispiel in anderen Regionen befinden können. Es genügt, wenn in jedem Segment des Netzwerks ein sekundärer Administrationsserver installiert ist, die Geräte auf Administrationsgruppen der sekundären Server verteilt werden und für die sekundären Server schnelle Verbindungen zum primären Server bestehen.

- Verteilung der Verantwortung zwischen den Administratoren für den Antiviren-Schutz. Dabei bleiben alle Möglichkeiten der zentralen Verwaltung und der Überwachung des Status des Antiviren-Schutzes im Unternehmensnetzwerk erhalten.

- Verwendung von Kaspersky Security Center über Dienstanbieter. Ein Dienstanbieter muss lediglich Kaspersky Security Center und die Kaspersky Security Center Web Console installieren. Um eine große Anzahl an Client-Geräten verschiedener Unternehmen zu verwalten, kann der Dienstanbieter sekundäre Administrationsserver (einschließlich sekundärer Server) zur Hierarchie der Administrationsserver hinzufügen.

Jedes Gerät, das zur Hierarchie der Administrationsgruppen gehört, kann nur mit einem Administrationsserver verbunden sein. Sie müssen die Verbindung der Geräte mit den Administrationsservern selbständig prüfen. Dazu können Sie die Suche-Funktion der Geräte nach Netzwerkattributen in den Administrationsgruppen verschiedener Server verwenden.

Virtueller Administrationsserver

Ein virtueller Administrationsserver (im Folgenden auch *virtueller Server* genannt) ist eine Komponente von Kaspersky Security Center Linux, die dazu dient, den Antiviren-Schutz im Netzwerk eines Kundenunternehmens zu verwalten.

Ein virtueller Administrationsserver stellt einen besonderen Fall eines sekundären Administrationsservers dar und weist im Vergleich zu einem physikalischen Administrationsserver folgende Einschränkungen auf:

- Ein virtueller Administrationsserver kann nur auf einem primären Administrationsserver erstellt werden.
- Ein virtueller Administrationsserver verwendet während seines Betriebs die Datenbank des primären Administrationsservers. Aufgaben zum Anlegen eines Daten-Backups und zur Wiederherstellung von Dateien, sowie Aufgaben zur Suche nach Updates und Downloadaufgaben werden von einem virtuellen Administrationsserver nicht unterstützt.
- Für virtuelle Server können keine sekundären Administrationsserver angelegt werden (einschließlich virtueller Server).

Außerdem weisen virtuelle Administrationsserver folgende Einschränkungen auf:

- Im Eigenschaftenfenster des virtuellen Administrationsservers ist die Anzahl der Abschnitte beschränkt.
- Um eine Remote-Installation von Kaspersky-Anwendungen auf Client-Geräten vorzunehmen, die vom virtuellen Administrationsserver verwaltet werden, muss auf einem der Computer der Administrationsagent installiert sein, über den eine Verbindung zum virtuellen Administrationsserver aufgebaut werden kann. Beim ersten Verbindungsaufbau zum virtuellen Administrationsserver wird diesem Computer automatisch die Rolle des Verteilungspunkts zugewiesen, sodass er als Verbindungs-Gateway für den Anschluss von Client-Geräten an den virtuellen Administrationsserver dient.
- Der virtuelle Server kann das Netzwerk nur über die Verteilungspunkte durchsuchen.
- Um einen nicht voll funktionsfähigen virtuellen Server neu zu starten, startet Kaspersky Security Center Linux den primären Administrationsserver und alle virtuellen Administrationsserver neu.
- Benutzern, die auf einem virtuellen Server erstellt wurden, können auf dem Administrationsserver keine Rollen zugewiesen werden.

Der Administrator eines virtuellen Administrationsservers verfügt über alle Rechte für diesen virtuellen Server.

Webserver

Beim Kaspersky Security Center *Webserver* (im Folgenden auch *Webserver* genannt) handelt es sich um eine Kaspersky Security Center Komponente, die zusammen mit dem Administrationsserver installiert wird. Der Webserver dient dazu, autonome Installationspakete und Dateien aus einem freigegebenen Ordner im Netzwerk zu übertragen.

Beim Erstellen wird ein autonomes Installationspaket automatisch auf dem Webserver veröffentlicht. Der Link für den Download des autonomen Paketes wird in der Liste der erstellten autonomen Installationspakete angezeigt. Bei Bedarf können Sie die Veröffentlichung des autonomen Paketes abbrechen oder es erneut auf dem Webserver veröffentlichen.

Der freigegebene Ordner wird zum Speichern von Informationen verwendet, die für alle Benutzer verfügbar sind, deren Geräte über den Administrationsserver verwaltet werden. Hat ein Benutzer keinen direkten Zugriff auf den freigegebenen Ordner, können die Informationen aus diesem Ordner mithilfe des Webservers an ihn übermittelt werden.

Um Informationen aus dem freigegebenen Ordner mithilfe des Webservers an Benutzer übermitteln zu können, soll der Administrator im Ordner einen Unterordner mit dem Namen public erstellen und die Informationen in diesen Unterordner kopieren.

Der Link für die Übermittlung der Informationen an den Benutzer soll folgendes Aussehen aufweisen:

```
https://<Web Server name>:<HTTPS port>/public/<object>
```

wobei:

- `<Web Server name>` für den Namen des Kaspersky Security Center Webservers.
- `<HTTPS port>` für den vom Administrator angegebenen HTTPS-Port des Webservers steht. Den HTTPS-Port können Sie im Abschnitt **Webserver** im Eigenschaftenfenster des Administrationsservers festlegen. Standardmäßig wird Portnummer 8061 verwendet.
- Beim `<object>` handelt es sich um einen Unterordner bzw. eine Datei, die für den Benutzer freigegeben werden sollen.

Der Administrator kann den erstellten Link auf jede Weise an den Benutzer übermitteln, wie etwa per E-Mail.

Mit diesem Link kann der Benutzer die für ihn vorgesehenen Informationen auf das lokale Gerät herunterladen.

Kaspersky Security Center Linux Webserver

Kaspersky Security Center Linux Webserver (im Folgenden "Webserver") ist eine Komponente von Kaspersky Security Center Linux. Der Webserver ermöglicht die Veröffentlichung von autonomen Installationspaketen und von Dateien aus dem freigegebenen Ordner.

Die erstellten Installationspakete werden automatisch auf dem Webserver veröffentlicht und nach dem ersten Download gelöscht. Der Administrator kann den erstellten Link auf beliebige Weise an den Benutzer übermitteln, z. B. per E-Mail.

Über diesem Link kann der Benutzer die für erforderlichen Informationen auf ein mobiles Gerät herunterladen.

Webserver-Einstellungen

Wenn Sie den Webserver noch genauer anpassen möchten, können Sie in den Webserver-Eigenschaften die Ports für die Protokolle HTTP (8060) und HTTPS (8061) ändern. Zudem können Sie auch das Serverzertifikat für das HTTPS-Protokoll ersetzen und den FQDN-Namen des Webservers für das HTTP-Protokoll ändern.

Webserver-Einstellungen auf einem Verbindungs-Gateway

Auf einem Verteilungspunkt im Modus "Verbindungs-Gateway" wird ein separater Webserver-Dienst implementiert, der die Verwendung von mobilen Geräten ermöglicht, die mit Kaspersky Security Center Linux verbunden sind. Dieser Dienst überträgt Installationspakete für Anwendungen und Profile zur Geräteverwaltung an Geräte, ohne diese Geräte direkt mit dem Administrationsserver zu verbinden. Die Daten werden übertragen, indem der Dienst HTTP-/HTTPS-Dateianforderungen auf dem Verbindungsgateway verarbeitet.

Der Webserver-Dienst auf einem Verbindungs-Gateway wird zusammen mit dem Administrationsagenten für Linux installiert. Um diese Funktion zu verwenden, müssen Sie ein Gerät zuweisen, das im Verbindungs-Gateway-Modus als Verteilungspunkt fungiert und als Webserver verwendet wird. Anschließend müssen Sie die entsprechenden Einstellungen angeben. Ausführliche Informationen zur Konfiguration der Webserver-Einstellungen auf einem Verbindungs-Gateway finden Sie in der Hilfe zu Kaspersky Secure Mobility Management.

Administrationsagent

Interaktion zwischen dem Administrationsserver und Geräten wird mithilfe der Komponente *Administrationsagent* von Kaspersky Security Center Linux durchgeführt. Der Administrationsagent muss auf allen Geräten installiert werden, auf welchen Kaspersky-Anwendungen mit Kaspersky Security Center Linux verwaltet werden.

Ein Gerät, auf dem der Administrationsagent installiert ist, wird als *verwaltetes Gerät* oder *Gerät* bezeichnet. Sie können das Installationspaket des Administrationsagenten aus den folgenden Quellen herunterladen:

- Speicher des Administrationsservers (es muss ein Administrationsserver installiert sein)
- Kaspersky-Website

Der Administrationsagent für Linux wird auf dem Gerät als Dienst mit den folgenden Attributen installiert:

- Besitzt den Namen "Kaspersky Administrationsagent"
- Mit automatischem Start bei Start des Betriebssystems
- Unter Verwendung des Kontos "root"

Der Administrationsagent für Windows wird auf dem Gerät als Dienst mit den folgenden Attributen installiert:

- Besitzt den Namen "Kaspersky Security Center Administrationsagent"
- Mit automatischem Start bei Start des Betriebssystems
- Unter Verwendung des Kontos "LocalSystem"

Der Administrationsagent für macOS wird auf dem Gerät als Dienst mit den folgenden Attributen installiert:

- Besitzt den Namen "com.kaspersky.klnagent.core"
- Wird beim Starten des Betriebssystems automatisch gestartet
- Verwendet das "root"-Benutzerkonto

Die Namen der Dienstprozesse:

- Unter Linux:
  - klnagent64.service (für 64-Bit-Betriebssysteme)
  - klnagent.service (für 32-Bit-Betriebssysteme)
- Unter Windows:
  - klnagent
- Unter macOS:
  - com.kaspersky.klnagent

Standardmäßig wird der Administrationsagent an den folgenden Speicherorten installiert:

- Unter Linux:
  - 32-Bit-Systeme: /opt/kaspersky/klnagent/
  - 64-Bit-Systeme: /opt/kaspersky/klnagent64/
- Unter Windows:
  - 32-Bit-Systeme: C:\Programme\Kaspersky Lab\NetworkAgent
  - 64-Bit-Systeme: C:\Programme (x86)\Kaspersky Lab\NetworkAgent
- Unter macOS:
  - 64-Bit-Systeme: /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klnagent

Für Windows-Geräte können Sie in den Einstellungen des Installationspakets einen anderen Ordner für die Installation des Administrationsagenten angeben. Auf Linux-Geräten kann der Administrationsagent jedoch nur im Standardverzeichnis installiert werden.

Der Installationsordner des Administrationsagenten enthält mit Tools wie "klmover" und "klnagchk" auch Werkzeuge zur Verwaltung und Diagnose des Ausführungszustands des Administrationsagenten.

Bei der Installation des Administrationsservers wird die Serverversion des Administrationsagenten automatisch zusammen mit dem Administrationsserver installiert. Um jedoch das Gerät des Administrationsservers wie jedes andere verwaltete Gerät zu verwalten zu können, installieren Sie den Administrationsagenten für Linux auf dem Gerät des Administrationsservers. In diesem Fall wird der Administrationsagent für Linux installiert und funktioniert unabhängig von der Serverversion des Administrationsagenten, die Sie zusammen mit dem Administrationsserver installiert haben.

Der Administrationsagent synchronisiert das verwaltete Gerät mit dem Administrationsserver. Es wird empfohlen, das Synchronisierungsintervall (auch als *Herzschlag* bezeichnet) auf 15 Minuten pro 10.000 verwaltete Geräte einzurichten.

Administrationsgruppen

Bei einer *Administrationsgruppe* (im Folgenden *Gruppe* genannt) handelt es sich um einen logischen Satz von verwalteten Geräte, die nach einem beliebigen Merkmal zusammengefasst sind und als geschlossene Einheit innerhalb von Kaspersky Security Center Linux verwaltet werden können.

Alle verwalteten Geräte innerhalb einer Administrationsgruppe sind für folgende Aktionen konfiguriert:

- Verwenden derselben Anwendungseinstellungen (die Sie in Gruppenrichtlinien festlegen können).
- Verwenden eines allgemeinen Betriebsmodus für alle Anwendungen, indem Gruppenaufgaben mit festgelegten Einstellungen erstellt werden. Beispiele für Gruppenaufgaben umfassen unter anderem das Erstellen und Installieren eines Standard-Installationspakets, Aktualisieren von Datenbanken und Modulen von Anwendungen, Untersuchung des Geräts auf Befehl und Aktivieren des Echtzeitschutzes.

Ein verwaltetes Gerät kann nur zu einer Administrationsgruppe gehören.

Sie können Hierarchien erstellen, die einen beliebige Tiefe für die Verschachtelung der Administrationsserver und der Gruppen aufweisen. Auf einer Hierarchieebene können sich sekundäre und virtuelle Administrationsserver sowie Gruppen und verwaltete Geräte befinden. Sie können Geräte von einer Gruppe zu einer anderen verschieben, ohne sie physikalisch zu bewegen. Wenn sich beispielsweise die Position eines Mitarbeiters im Unternehmen von Buchhalter auf Entwickler ändert, können Sie das Gerät dieses Mitarbeiters von der Administrationsgruppe "Buchhalter" in die Administrationsgruppe "Entwickler" verschieben. Anschließend erhält das Gerät automatisch die Programmeinstellungen, die für Entwickler erforderlich sind.

Verwaltetes Gerät

Ein *verwaltetes Gerät* ist ein Gerät, auf dem Linux, Windows oder macOS ausgeführt wird und auf dem der Administrationsagent installiert ist. Sie können solche Geräte verwalten, indem Sie Aufgaben und Richtlinien für auf diesen Geräten installierte Anwendungen erstellen. Sie können auch Berichte von verwalteten Geräten beziehen.

Sie können ein verwaltetes Gerät als Verteilungspunkt und als Verbindungs-Gateway nutzen.

Ein Gerät kann nur von einem Administrationsserver verwaltet werden. Die Anzahl der Geräte, die von einem Administrationsserver verwaltet werden können, hängt sowohl von der Konfiguration des Geräts mit installiertem Administrationsserver als auch von den DBMS-Beschränkungen ab.

Nicht zugeordnetes Gerät

Ein *nicht zugeordnetes Gerät* ist ein Gerät im Netzwerk, dass in keine Administrationsgruppe aufgenommen wurde. Sie können mit den nicht zugeordneten Geräten Aktionen ausführen und sie z. B. in Administrationsgruppen verschieben oder Anwendungen darauf installieren.

Wenn ein neues Gerät in Ihrem Netzwerk gefunden wird, gelangt dieses Gerät in die Administrationsgruppe **Nicht zugeordnete Geräte**. Sie können Regeln für Geräte anpassen, die automatisch in andere Administrationsgruppen verschoben werden sollen, nachdem die Geräte ermittelt wurden.

Administrator-Arbeitsplatz

Geräte, auf denen der Server der Web Console von Kaspersky Security Center installiert ist, werden als *Administrator-Arbeitsplätze* bezeichnet. Von diesen Geräten aus können die Administratoren eine zentralisierte Remote-Programmverwaltung für die auf den Client-Geräten installierten Kaspersky-Anwendungen durchführen.

Die Anzahl an Administrator-Arbeitsplätzen ist nicht beschränkt. Von jedem Administrator-Arbeitsplatz aus können die Administrationsgruppen mehrerer Administrationsserver des Netzwerks verwaltet werden. Der Administrator-Arbeitsplatz kann mit dem Administrationsserver (physischen oder virtuellen) einer beliebigen Hierarchieebene verbunden werden.

Der Administrator-Arbeitsplatz kann in eine Administrationsgruppe als Client-Gerät aufgenommen werden.

Im Rahmen von Administrationsgruppen eines beliebigen Servers kann dasselbe Gerät sowohl Client des Administrationsservers als auch Administrationsserver und Administrator-Arbeitsplatz sein.

Web-Plug-ins zur Verwaltung

Für die Remote-Verwaltung der Software von Kaspersky mithilfe von Kaspersky Security Center Web Console wird eine spezielle Komponente – das *Web-Plug-in zur Verwaltung* – verwendet. Im Weiteren wird das Web-Plug-in zur Verwaltung als *Verwaltungs-Plug-in* bezeichnet. Das Verwaltungs-Plug-in ist eine Schnittstelle zwischen Kaspersky Security Center Web Console und einer spezifischen Kaspersky-Anwendung. Mit einem Verwaltungs-Plug-in können Sie Aufgaben und Richtlinien für die Anwendung konfigurieren.

Sie können die Web-Plug-ins zur Verwaltung von der Kaspersky-Website herunterladen.

Das Verwaltungs-Plug-in stellt Folgendes bereit:

- Schnittstelle zum Erstellen und Ändern von Aufgaben und Einstellungen für Anwendungen
- Schnittstelle zum Erstellen und Ändern von Richtlinien und Richtlinienprofilen für die ferngesteuerte und zentralisierte Konfiguration von Kaspersky-Anwendungen und Geräten
- Übertragung von Ereignissen, die von der Anwendung erzeugt wurden
- Kaspersky Security Center Web Console funktioniert für die Anzeige von Betriebsdaten und Ereignissen der Anwendung sowie von Statistiken, die von Client-Geräten weitergeleitet wurden

Richtlinien

Eine *Richtlinie* besteht aus einer Reihe von Einstellungen für Kaspersky-Anwendungen, die auf eine Administrationsgruppe und deren Untergruppen angewendet werden. Sie können mehrere Kaspersky-Anwendungen auf den Geräten einer Administrationsgruppe installieren. Kaspersky Security Center bietet eine einzelne Richtlinie für jede Kaspersky-Anwendung in einer Administrationsgruppe. Eine Richtlinie hat eine der folgenden Statusvarianten:

Status der Richtlinie

Status	Beschreibung
Aktiv	Die aktuelle Richtlinie, die auf das Gerät angewendet wird. In jeder Administrationsgruppe kann nur eine Richtlinie für eine Kaspersky-Anwendung aktiv sein. Geräte wenden die Einstellungswerte einer aktiven Richtlinie für eine Kaspersky-Anwendung an.
Inaktiv	Eine Richtlinie, die derzeit nicht auf ein Gerät angewendet wird.
Für mobile Benutzer	Bei Auswahl dieser Option wird die Richtlinie aktiv, sobald das Gerät vom Unternehmensnetzwerk getrennt wird.

Richtlinien funktionieren gemäß den folgenden Regeln:

- Für eine einzelne Anwendung können mehrere Richtlinien mit unterschiedlichen Werten konfiguriert werden.
- Für die aktuelle Anwendung kann nur eine Richtlinie aktiv sein.
- Eine Richtlinie kann untergeordnete Richtlinien haben.

Im Allgemeinen können Sie Richtlinien als Vorbereitung für Notfallsituationen wie Virenangriffe verwenden. Beispiel: Wenn ein Angriff über Flash-Laufwerke erfolgt, können Sie eine Richtlinie aktivieren, die den Zugriff auf Flash-Laufwerke blockiert. In diesem Fall wird die aktuell aktive Richtlinie automatisch inaktiv.

Um zu verhindern, dass mehrere Richtlinien verwaltet werden, können Sie beispielsweise Richtlinienprofile verwenden, wenn bei verschiedenen Gelegenheiten nur bestimmte Einstellungen geändert werden müssen.

Ein *Richtlinienprofil* stellt eine benannte Teilmenge von Einstellungswerten einer Richtlinie dar, welche die Einstellungswerte in einer Richtlinie ersetzen. Ein Richtlinienprofil wirkt sich auf die effektive Formation der Einstellungen auf einem verwalteten Gerät aus. *Effektive Einstellungen* stellen eine Zusammenstellung an Einstellungen für Richtlinien, Richtlinienprofile und lokalen Anwendungseinstellungen dar, die derzeit für das Gerät angewendet werden.

Richtlinienprofile funktionieren entsprechend den folgenden Regeln:

- Ein Richtlinienprofil wird wirksam, wenn eine bestimmte Aktivierungsbedingung erfüllt ist.
- Richtlinienprofile enthalten Werte für Einstellungen, die von den Richtlinieneinstellungen abweichen.
- Durch das Aktivieren eines Richtlinienprofils werden die effektiven Einstellungen des verwalteten Gerätes geändert.
- Eine Richtlinie kann nicht mehr als 100 Richtlinienprofile enthalten.

Richtlinienprofile

Es kann manchmal erforderlich werden, in verschiedenen Administrationsgruppen mehrere Instanzen einer einzigen Richtlinie zu erstellen. Bei Bedarf können Sie die Einstellungen dieser Richtlinien auch zentral bearbeiten. Diese Instanzen können sich nur durch ein oder zwei Einstellungen unterscheiden. Beispielsweise arbeiten alle Buchhalter in einem Unternehmen unter derselben Richtlinie, leitende Buchhalter dürfen jedoch USB-Flash-Drives verwenden, was reguläre Buchhalter nicht dürfen. In diesem Fall ist die Übernahme von Richtlinien für Geräte ausschließlich gemäß der Hierarchie von Administrationsgruppen möglicherweise unpraktisch.

Damit Sie nicht mehrere Instanzen einer einzelnen Richtlinie erstellen müssen, ermöglicht es Ihnen Kaspersky Security Center Linux, *Richtlinienprofile* zu erstellen. Richtlinienprofile sind erforderlich, wenn Sie möchten, dass Geräte innerhalb einer Administrationsgruppe unter verschiedenen Richtlinieneinstellungen ausgeführt werden.

Ein Richtlinienprofil ist eine benannte Teilmenge von Richtlinieneinstellungen. Diese Teilmenge wird auf Zielgeräten gemeinsam mit der Richtlinie verteilt und ergänzt sie unter einer bestimmten Bedingung, die als *Profilaktivierungsbedingung* bezeichnet wird. Profile enthalten nur jene Einstellungen, die sich von der "zugrundeliegenden" Richtlinie unterscheiden, die auf dem verwalteten Gerät aktiv ist. Die Aktivierung eines Profils ändert die Einstellungen der "zugrundeliegenden" Richtlinie, die ursprünglich auf dem Gerät aktiv waren. Die geänderten Einstellungen nehmen die im Profil festgelegten Werte an.

Aufgaben

Kaspersky Security Center Linux verwaltet die auf Geräten installierten Sicherheitsanwendungen von Kaspersky durch das Erstellen und Starten von *Aufgaben*. Die Aufgaben ermöglichen Installation, Start und Beenden von Anwendungen, Untersuchung von Dateien, Datenbanken-Update und Aktualisierung der Anwendungsmodule sowie Ausführung anderer Aktionen mit den Anwendungen.

Aufgaben für eine bestimmte Anwendung können nur erstellt werden, sofern das Verwaltungs-Plug-in für diese Anwendung installiert ist.

Aufgaben können auf dem Administrationsserver und auf Geräten ausgeführt werden.

Die folgenden Aufgaben werden auf dem Administrationsserver ausgeführt:

- Berichte automatisch versenden
- Updates in die Datenverwaltung des Administrationsservers herunterladen
- Backup der Daten des Administrationsservers anlegen
- Datenbank bedienen

Die folgenden Typen von Aufgaben werden auf Geräten ausgeführt:

- *Lokale Aufgaben* sind Aufgaben, die auf einem bestimmten Gerät ausgeführt werden.

  Lokale Aufgaben können nicht nur vom Administrator mithilfe von Kaspersky Security Center Web Console geändert werden, sondern auch vom Benutzer des Remote-Gerätes (beispielsweise in der Benutzeroberfläche der Sicherheits-Anwendungen). Wenn eine lokale Aufgabe gleichzeitig sowohl vom Administrator als auch vom Benutzer auf dem verwalteten Gerät geändert wurde, treten jene Änderungen in Kraft, die vom Administrator mit höherer Priorität ausgeführt wurden.

- *Gruppenaufgaben* sind Aufgaben, die auf allen Geräten einer bestimmten Gruppe ausgeführt werden.

  Soweit in den Aufgabeneigenschaften nicht anders festgelegt, betrifft eine Gruppenaufgabe auch alle Untergruppen der ausgewählten Gruppe. Eine Gruppenaufgabe betrifft (optional) auch Geräte, die mit den sekundären und virtuellen Administrationsservern in der Gruppe und den Untergruppen verbunden sind.

- *Globale Aufgaben* sind Aufgaben, die auf einem Satz von Geräten ausgeführt werden, und zwar unabhängig davon, ob sie zu einer Gruppe gehören.

Sie können für jede Anwendung eine beliebige Anzahl von Gruppenaufgaben, globalen Aufgaben oder lokalen Aufgaben erstellen.

Sie können die Aufgabeneinstellungen ändern, den Fortschritt von Aufgaben verfolgen, und Aufgaben kopieren, exportieren, importieren und löschen.

Eine Aufgabe wird auf einem Gerät nur dann gestartet, wenn die Anwendung gestartet wurde, für das diese Aufgaben erstellt worden waren.

Ergebnisse von Aufgaben werden im Syslog-Ereignisprotokoll und im Ereignisprotokoll von Kaspersky Security Center Linux sowohl zentral auf dem Administrationsserver als auch lokal auf jedem Gerät gespeichert.

Geben Sie in den Einstellungen der Aufgaben keine vertraulichen Daten an. Dazu gehört z. B. das Kennwort des Domänenadministrators.

Aufgabenumfang

Der *Gültigkeitsbereich einer Aufgabe* ist die Menge von Geräten, auf denen die Aufgabe ausgeführt wird. Es gibt folgende Arten von Gültigkeitsbereichen:

- Für eine *lokale Aufgabe* ist der Gültigkeitsbereich das Gerät selbst.
- Für eine *Aufgabe des Administrationsservers* ist der Gültigkeitsbereich der Administrationsserver.
- Für eine *Gruppenaufgabe* ist der Gültigkeitsbereich die Liste der Geräte, die in der Gruppe enthalten sind.

Beim Erstellen einer *globalen Aufgabe* können Sie die folgenden Methoden verwenden, um ihren Gültigkeitsbereich festzulegen:

- Bestimmte Geräte manuell festlegen.

  Als Adresse des Gerätes können Sie eine IP-Adresse (oder einen IP-Bereich) oder einen DNS-Namen verwenden. Sie können auch Netzwerkgeräte auswählen, die vom Administrationsserver erkannt wurden.

- Geräteliste aus einer txt-Datei mit den hinzuzufügenden Geräteadressen importieren (jede Adresse muss in einer eigenen Zeile stehen).

  Wenn Sie eine Geräteliste aus einer Datei importieren oder eine Liste manuell erstellen, und wenn die Geräte namentlich identifiziert werden, darf die Liste nur Geräte enthalten, deren Daten bereits in die Administrationsserver-Datenbank eingegeben wurden. Darüber hinaus müssen die Informationen entweder während einer bestehenden Verbindung der Geräte oder während einer Gerätesuche eingegeben worden sein.

- Geräteauswahl angeben.

  Im Laufe der Zeit ändert sich der Gültigkeitsbereich der Aufgabe, je nachdem, wie sich die Anzahl der Geräte ändert, die zur Auswahl gehören. Die Geräteauswahl kann aufgrund der Geräte-Attribute, einschließlich aufgrund der auf dem Gerät installierten Software, und aufgrund der dem Gerät zugewiesenen Tags strukturiert sein. Die Geräteauswahl ist die flexibelste Art zum Festlegen des Gültigkeitsbereichs einer Aufgabe.

  Aufgaben für die Geräteauswahlen werden immer nach Zeitplan durch den Administrationsserver ausgeführt. Solche Aufgaben werden auf Geräten, die keine Verbindung mit dem Administrationsserver haben, nicht ausgeführt. Aufgaben, deren Gültigkeitsbereich mithilfe anderer Methoden festgelegt ist, werden direkt auf Geräten ausgeführt und sind daher nicht von der Geräteverbindung zum Administrationsserver abhängig.

  Aufgaben für Geräteauswahlen werden nicht nach der lokalen Uhrzeit des Geräts, sondern nach der lokalen Uhrzeit des Administrationsservers ausgeführt. Aufgaben, deren Gültigkeitsbereich mithilfe anderer Methoden festgelegt ist, werden nach der lokalen Uhrzeit eines Geräts ausgeführt.

Interaktion von Richtlinien und lokalen Programmeinstellungen

Mit Richtlinien können identische Werte für Einstellungen einer Anwendung für alle Geräte gesetzt werden, die zu einer Gruppe gehören.

Die Einstellungswerte, die eine Richtlinie vorgibt, lassen sich für einzelne Geräte mit lokalen Anwendungseinstellungen ändern. Dabei können Werte nur für die Einstellungen festgelegt werden, deren Änderung nicht durch die Richtlinie unterbunden ist, d.h. wenn die Einstellung nicht durch ein verriegeltes Schloss blockiert wird.

Der Wert, den die Anwendung auf dem Client-Gerät verwendet wird durch die Position des Schlosses (🔒) für diese Richtlinieneinstellung definiert:

- Wenn die Änderung der Einstellung unterbunden ist, wird auf allen Client-Geräten der gleiche Wert verwendet, der von der Richtlinie vorgegeben ist.
- Wenn die Änderung nicht unterbunden ist, verwendet die Anwendung den lokalen Einstellungswert auf jedem Client-Gerät und nicht den Wert, der in der Richtlinie angegeben ist. Der Einstellungswert kann dabei über die lokalen Anwendungseinstellungen geändert werden.

Dies bedeutet, das bei Ausführung einer Aufgabe auf dem Client-Gerät die Anwendung Einstellungen anwendet, die auf zwei verschiedene Arten vorgegeben wurden:

- Durch die Aufgabeneinstellungen und die lokalen Anwendungseinstellungen, wenn die Änderung der Einstellung in der Richtlinie nicht unterbunden wurde.
- Durch die Gruppenrichtlinie, wenn die Änderung der Einstellung gesperrt wurde.

Die lokalen Anwendungseinstellungen werden nach der ersten Anwendung der Richtlinie mit den Richtlinieneinstellungen überschrieben.

Verteilungspunkt

Der *Verteilungspunkt* (bisher "Update-Agent") ist ein Gerät mit installiertem Administrationsagenten, das verwendet wird für die Update-Verteilung, die Remote-Installation von Anwendungen und den Empfang von Informationen über Geräte im Netzwerk.

> Die Funktionen und Anwendungsfälle eines Administrationsagenten, der auf einem Gerät installiert ist, das als Verteilungspunkt fungiert variieren je nach Betriebssystem.

Der Verteilungspunkt kann folgende Funktionen ausführen:

- Updates und Installationspakete, die vom Administrationsserver heruntergeladen wurden, auf die Client-Geräte der Gruppe verteilen (einschließlich Verteilung durch Multicasting über das UDP-Protokoll). Updates können sowohl vom Administrationsserver als auch von den Kaspersky-Update-Servern empfangen werden. Im letzteren Fall muss für den Verteilungspunkt eine Update-Aufgabe erstellt werden.

  Verteilungspunkte beschleunigen die Update-Verteilung und ermöglichen, die Belastung des Administrationsservers zu verringern.

- Verteilen von Richtlinien und Gruppenaufgaben mittels Multicast über das UDP-Protokoll.

- Rolle des Gateways für die Verbindung mit dem Administrationsserver für Geräte in einer Administrationsgruppe übernehmen.

  Wenn keine Möglichkeit besteht, eine direkte Verbindung zwischen den verwalteten Geräten und dem Administrationsserver herzustellen, können Sie den Verteilungspunkt zum Gateway für Verbindungen dieser Gruppe mit dem Administrationsserver bestimmen. In diesem Fall werden die verwalteten Geräte mit dem Verbindungs-Gateway verbunden, das seinerseits mit dem Administrationsserver verbunden wird.

  Das Vorhandensein eines Verteilungspunkts, der die Rolle des Verbindungs-Gateways übernimmt, schließt eine direkte Verbindung der verwalteten Geräte mit dem Administrationsserver nicht aus. Wenn das Verbindungs-Gateway nicht verfügbar ist, aber eine direkte Verbindung mit dem Administrationsserver möglich ist, werden die verwalteten Geräte direkt mit dem Server verbunden.

- Abfragen des Netzwerks, um neue Geräte und aktualisierte Informationen über die bereits bekannten Geräte zu finden. Der Verteilungspunkt kann dieselben Methoden zur Gerätesuche ausführen wie der Administrationsserver.

- Remote-Installation von Kaspersky-Anwendungen und von Anwendungen anderer Softwareanbietern, einschließlich der Installation auf Client-Geräten ohne Administrationsagent.

  Diese Funktion ermöglicht es, Installationspakete des Administrationsagenten auf Client-Geräte zu übertragen, die sich in Netzwerken befinden, auf die der Administrationsserver nicht direkt zugreifen kann.

- Als Proxyserver fungieren, der am Kaspersky Security Network (KSN) teilnimmt.

  Sie können den KSN-Proxyserver auf dem Verteilungspunkt aktivieren, damit das Gerät als KSN-Proxyserver agiert. In diesem Fall wird der KSN-Proxy-Service auf dem Gerät ausgeführt.

Die Übertragung von Dateien vom Administrationsserver an den Verteilungspunkt wird über das HTTP-Protokoll oder das HTTPS-Protokoll (wenn die Verwendung von SSL-Verbindungen konfiguriert ist) realisiert. Die Verwendung des HTTP- oder HTTPS-Protokolls gewährleistet im Vergleich zum SOAP-Protokoll aufgrund des reduzierten Datenverkehrs eine höhere Leistung.

Geräte mit installiertem Administrationsagenten können entweder manuell (vom Administrator) oder automatisch (vom Administrationsserver) als Verteilungspunkte bestimmt werden. Eine vollständige Liste der Verteilungspunkte für die angegebenen Administrationsgruppen wird im Bericht über die Liste der Verteilungspunkte angezeigt.

Der Gültigkeitsbereich des Verteilungspunkts umfasst die Administrationsgruppe, für die der Verteilungspunkt vom Administrator bestimmt wurde, sowie ihre Untergruppen auf jeder Ebene der Verschachtelung. Wurden in der Hierarchie der Administrationsgruppen mehrere Verteilungspunkte bestimmt, wird der Administrationsagent des verwalteten Geräts mit dem Verteilungspunkt verbunden, der sich in der Hierarchie am nächsten befindet.

Wenn die Verteilungspunkte automatisch vom Administrationsserver bestimmt werden, erfolgt dies anhand der Broadcast-Domänen und nicht anhand der Administrationsgruppen. Dies geschieht nachdem die Broadcast-Domäne bestimmt wurde. Der Administrationsagent führt einen Nachrichtenaustausch mit den anderen Administrationsagenten seines Subnetzes aus und sendet dem Administrationsserver Informationen über sich sowie Kurzinformationen über die anderen Administrationsagenten. Auf der Grundlage dieser Informationen kann der Administrationsserver eine Gruppierung der Administrationsagenten anhand der Broadcast-Domänen durchführen. Die Broadcast-Domänen werden dem Administrationsserver bekannt, nachdem mehr als 70 % der Administrationsagenten in den Administrationsgruppen durchsucht wurden. Der Administrationsserver durchsucht die Broadcast-Domänen alle zwei Stunden. Nachdem die Verteilungspunkte anhand der Broadcast-Domänen bestimmt wurden, können sie nicht mehr neu anhand von Administrationsgruppen bestimmt werden.

Wenn der Administrator die Verteilungspunkte manuell zuweist, können diese Verwaltungsgruppen oder Netzwerkstandorten zugewiesen werden.

Administrationsagenten mit einem aktiven Verbindungsprofil nehmen nicht an der Ermittlung der Broadcast-Domäne teil.

Kaspersky Security Center Linux weist jedem Administrationsagenten eine eindeutige Adresse für den IP-Versand an mehrere Adressen zu, die sich nicht mit anderen Adressen überschneidet. Dadurch kann eine Überschreitung der Netzwerkbelastung vermieden werden, die aufgrund der Überkreuzung von IP-Adressen entstehen könnte. Adressen für IP-Versand an mehrere Adressen, die schon in den vorigen Anwendungsversionen zugewiesen wurden, werden nicht geändert.

Wenn in einem Netzwerksegment oder einer Administrationsgruppe zwei oder mehr Verteilungspunkte bestimmt werden, wird einer davon aktiv, und die anderen bleiben in Reserve. Der aktive Verteilungspunkt lädt Updates und Installationspakete unmittelbar vom Administrationsserver herunter, während die Reserve-Verteilungspunkte nur den aktiven Verteilungspunkt nach Updates abfragen. In diesem Fall werden Dateien nur einmal vom Administrationsserver heruntergeladen und im Weiteren auf die Verteilungspunkte verteilt. Sollte der aktive Verteilungspunkt aus irgendwelchen Gründen offline sein, wird einer der Reserve-Verteilungspunkte zum aktiven bestimmt. Der Administrationsserver bestimmt die Reserve-Verteilungspunkte automatisch.

Der Status eines Verteilungspunkts (*Aktiv*/*Reserve*) wird mittels eines Kontrollkästchens im Bericht des Tools klnagchk angezeigt.

Für die Ausführung des Verteilungspunkts sind mindestens 4 GB freier Speicherplatz auf dem Datenträger erforderlich. Wenn der freie Speicherplatz auf dem Datenträger des Verteilungspunkts weniger als 2 GB beträgt, erstellt Kaspersky Security Center Linux einen Sicherheitsvorfall der Ereigniskategorie *Warnung*. Der Sicherheitsvorfall wird in den Eigenschaften des Geräts im Abschnitt **Sicherheitsprobleme** veröffentlicht.

Für die Ausführung von Aufgaben zur Remote-Installation ist auf dem Gerät mit dem Verteilungspunkt zusätzlicher freier Speicherplatz auf dem Datenträger erforderlich. Der freie Speicherplatz sollte größer sein als der Gesamtumfang aller zu installierenden Installationspakete.

Für die Ausführung der Aufgaben zur Installation von Updates (Patches) und zum Schließen von Schwachstellen ist auf dem Gerät mit dem Verteilungspunkt zusätzlicher freier Speicherplatz auf dem Datenträger erforderlich. Der freie Speicherplatz sollte mindestens doppelt so groß sein wie der Gesamtumfang aller zu installierenden Patches.

Geräte, die als Verteilungspunkte fungieren, müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Verbindungs-Gateway

Ein *Verbindungs-Gateway* ist ein Administrationsagent, der in einem speziellen Modus ausgeführt wird. Ein Verbindungs-Gateway akzeptiert Verbindungen von anderen Administrationsagenten und tunnelt diese zum Administrationsserver mittels einer eigenen Verbindung zum Server. Anstatt wie gewöhnliche Administrationsagenten selbst eine Verbindung zum Administrationsserver herzustellen, wartet ein Verbindungs-Gateway auf eine Verbindung vom Administrationsserver.

Ein Verbindungs-Gateway kann bis zu 10.000 Verbindungen von Geräten empfangen.

Sie haben zwei Möglichkeiten, Verbindungs-Gateways zu verwenden:

- Wir empfehlen, dass Sie ein Verbindungs-Gateway in einer entmilitarisierten Zone (DMZ) installieren. Für andere Administrationsagenten, die auf mobilen Geräten installiert sind, müssen Sie explizit eine Verbindung zum Administrationsserver über das Verbindungs-Gateway konfigurieren.

  Ein Verbindungs-Gateway ändert oder verarbeitet in keiner Weise Daten, die von Administrationsagenten an den Administrationsserver übertragen werden. Es schreibt darüber hinaus keinerlei Daten in einen Puffer und kann daher auch keine Daten von einem Administrationsagenten annehmen und zu einem späteren Zeitpunkt an den Administrationsserver weiterleiten. Wenn ein Administrationsagent versucht, über das Verbindungs-Gateway eine Verbindung zum Administrationsserver herzustellen, aber das Verbindungs-Gateway keine Verbindung zum Administrationsserver herstellen kann, wird dieses Gateway vom Administrationsagenten als nicht erreichbar angesehen. Alle Daten verbleiben auf dem Administrationsagenten (nicht auf dem Verbindungs-Gateway).

  Ein Verbindungs-Gateway kann keine Verbindung zum Administrationsserver über ein weiteres Verbindungs-Gateway herstellen. Das bedeutet, dass ein Administrationsagent nicht gleichzeitig ein Verbindungs-Gateway sein und ein Verbindungs-Gateway verwenden kann, um eine Verbindung zum Administrationsserver herzustellen.

  Alle Verbindungs-Gateways sind in der Liste der Verteilungspunkte in den Eigenschaften des Administrationsservers enthalten.

- Sie können Verbindungs-Gateways auch innerhalb des Netzwerks verwenden. Beispielsweise werden automatisch zugewiesene Verteilungspunkte auch zu Verbindungs-Gateways in ihrem eigenen Bereich. Innerhalb eines internen Netzwerks bieten Verbindungs-Gateways jedoch keinen wesentlichen Vorteil. Sie reduzieren die Anzahl der vom Administrationsserver empfangenen Netzwerkverbindungen, jedoch nicht das Volumen eingehender Daten. Auch ohne Verbindungs-Gateways können alle Geräte eine Verbindung zum Administrationsserver herstellen.

Virtuelle Administrationsserver

Im Rahmen des physischen Administrationsservers können mehrere virtuelle Administrationsserver erstellt werden, die in vieler Hinsicht sekundären Servern ähnlich sind. Im Vergleich zum Modell des geteilten Zugriffs, der auf den Listen der Zugriffskontrolle (ACL) beruht, ist das Modell der virtuellen Administrationsserver funktioneller und bietet eine hohe Stufe der Isolierung. Neben der eigenen Struktur der Administrationsgruppen für verwaltete Geräte mit Richtlinien und Aufgaben hat jeder virtuelle Administrationsserver auch eine eigene Gruppe von nicht zugeordneten Geräten, die über eigene Sätze von Berichten, Geräteauswahlen und Ereignissen, Installationspakete, Regeln zur Verschiebung von Geräten usw. verfügt. Die Funktionalität der virtuellen Administrationsserver kann sowohl von Dienstanbietern (xSP) zur maximalen Isolierung verschiedener Kunden voneinander, als auch von großen Unternehmen mit komplizierter Struktur und einer großen Anzahl von Administratoren verwendet werden.

Virtuelle Administrationsserver ähneln in vieler Hinsicht sekundären Administrationsservern, haben jedoch die folgenden Unterschiede:

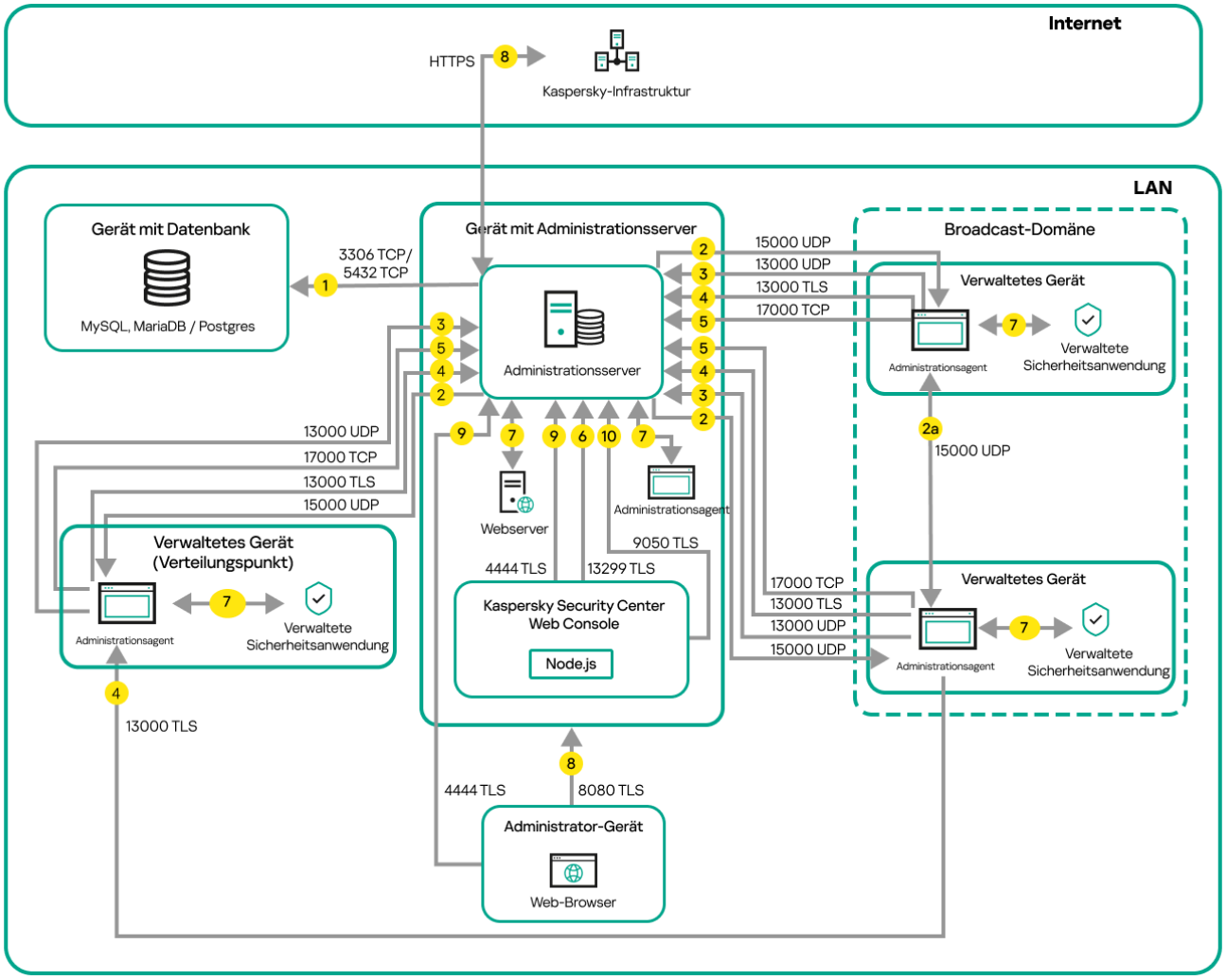
- Einem virtuellen Administrationsserver fehlt eine Vielzahl der globalen Einstellungen und eigenen TCP-Ports
- Ein virtueller Administrationsserver hat keine sekundären Administrationsserver
- Ein virtueller Administrationsserver kann keine eigenen virtuellen Administrationsserver haben
- Auf dem physischen Administrationsserver sind die Geräte, Gruppen, Ereignisse und Objekte der verwalteten Geräte (Elemente der Quarantäne, Programm-Registry und andere) aller seiner virtuellen Administrationsserver sichtbar
- Ein virtueller Administrationsserver kann das Netzwerk nur mittels der mit ihm verbundenen Verteilungspunkte abfragen

Schemata für Datenverkehr und Portnutzung

Dieser Abschnitt enthält Schemata für den Datenverkehr zwischen den Komponenten von Kaspersky Security Center Linux, den verwalteten Sicherheitsanwendungen und den externen Servern unter Berücksichtigung unterschiedlicher Konfigurationen. Die Schemata geben an, welche Ports auf den lokalen Geräten verfügbar sein müssen.

Administrationsserver und verwaltete Geräte im LAN

Die folgende Abbildung zeigt den Datenverkehr bei einer Verteilung von Kaspersky Security Center ausschließlich im lokalen Netzwerk (LAN).



Administrationsserver und verwaltete Geräte im lokalen Netzwerk (LAN)

Die Abbildung zeigt, wie verschiedene verwaltete Geräte auf unterschiedliche Arten mit dem Administrationsserver verbunden sind: Direkt oder über einen Verteilungspunkt. Verteilungspunkte verringern die Belastung auf dem Administrationsserver während der Update-Verteilung und optimieren den Netzwerkdatenverkehr. Verteilungspunkte werden jedoch nur benötigt, wenn die Anzahl an verwalteten Geräten entsprechend groß ist. Bei einer geringen Anzahl an verwalteten Geräten können alle Geräte die Updates direkt vom Administrationsserver empfangen.

Die Pfeile zeigen die Initiierung des Datenverkehrs an: Jeder Pfeil zeigt von einem Gerät, dass die Verbindung aufbaut, zu dem Gerät, dass auf die Anfrage antwortet. Die Portnummer und der Name des für die Datenübermittlung verwendeten Protokolls sind angegeben. Jeder Pfeil ist mit einer Zahl beschriftet, und für den entsprechenden Datenverkehr gilt:

1. Administrationsserver sendet Daten an die Datenbank. Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server und MariaDB Server oder Port 5432 für PostgreSQL Server oder Postgre Pro Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

2. Kommunikationsanfragen vom Administrationsserver werden über den UDP-Port 15000 an alle nicht-mobilen verwalteten Geräte gesendet.

   Administrationsagenten innerhalb einer Broadcast-Domäne senden sich gegenseitig Anfragen. Die Daten werden dann an den Administrationsserver gesendet und dazu verwendet, die Grenzen der Broadcast-Domäne zu definieren und Verteilungspunkte automatisch zuzuweisen (sofern diese Option aktiviert ist).

   Wenn der Administrationsserver keinen direkten Zugriff auf die verwalteten Geräte hat, werden keine direkten Kommunikationsanfragen vom Administrationsserver an diese Geräte gesendet.

   2a. Die Administrationsagenten von nicht mobilen verwalteten Geräten tauschen Daten über andere Administrationsagenten innerhalb derselben Broadcasting-Domäne aus (die Daten werden anschließend an den Administrationsserver gesendet).

3. Informationen über das Herunterfahren verwalteter Geräte werden über den UDP-Port 13000 vom Administrationsagenten an den Administrationsserver übermittelt.

4. Der Administrationsserver empfängt Verbindungen von Administrationsagenten und von sekundären Administrationsservern über den TLS-Port 13000.

   Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den Nicht-TLS-Port 14000 annehmen. Kaspersky Security Center unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den TLS-Port 13000 zu verwenden.

5. Die verwalteten Geräte (mit Ausnahme von mobilen Geräten) fordern die Aktivierung über den TCP-Port 17000 an. Das ist nicht erforderlich, wenn das Gerät einen eigenen Internetzugang hat, da das Gerät in einem solchen Fall die Daten direkt über das Internet an die Kaspersky-Server sendet.

6. Der Server der Web Console von Kaspersky Security Center sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

   Die Komponente Identitäts- und Zugriffsverwaltung (IAM) verbindet sich über TLS-Port 13299 mit dem Administrationsserver.

7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

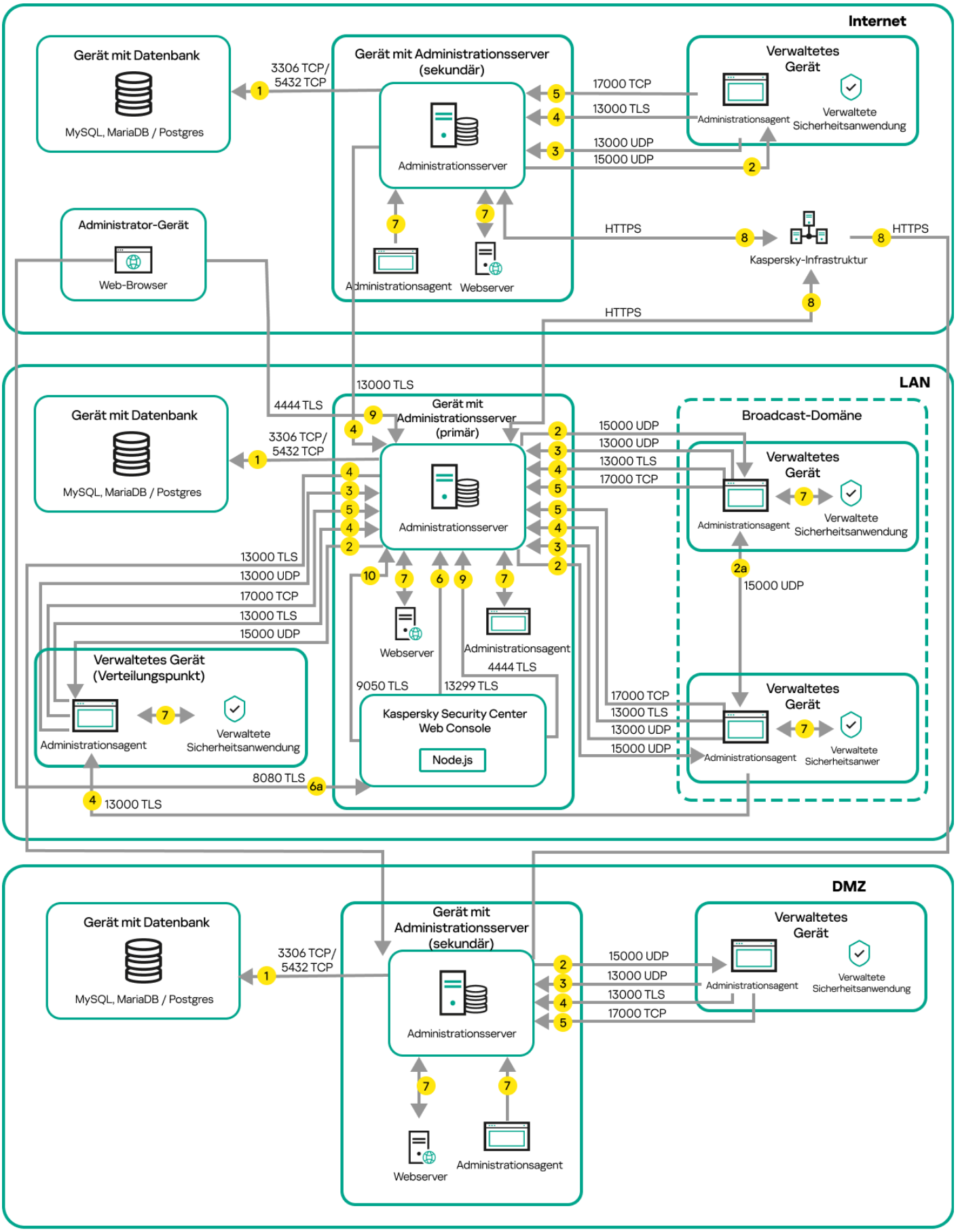
   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

9. Der Server der Kaspersky Security Center Web Console und der Browser (in dem die Kaspersky Security Center Web Console verwendet wird) verbinden sich mit dem Administrationsserver über das OpenID Connect-Authentifizierungsprotokoll durch TLS-Port 4444.

10. Der Server der Kaspersky Security Center Web Console verbindet sich mit dem Administrationsserver über den TLS-Port 9050.

Primärer Administrationsserver im LAN und zwei sekundäre Administrationsserver

Die folgende Abbildung zeigt die Hierarchie der Administrationsserver an: der primäre Administrationsserver befindet sich im lokalen Netzwerk (LAN). Ein sekundärer Administrationsserver befindet sich in der demilitarisierten Zone (DMZ) und ein weiterer sekundärer Administrationsserver im Internet.



Hierarchie der Administrationsserver: primärer Administrationsserver und zwei sekundäre Administrationsserver

Die Pfeile zeigen die Initiierung des Datenverkehrs an: Jeder Pfeil zeigt von einem Gerät, dass die Verbindung aufbaut, zu dem Gerät, dass auf die Anfrage antwortet. Die Portnummer und der Name des für die Datenübermittlung verwendeten Protokolls sind angegeben. Jeder Pfeil ist mit einer Zahl beschriftet, und für den entsprechenden Datenverkehr gilt:

1. Administrationsserver sendet Daten an die Datenbank. Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server und MariaDB Server oder Port 5432 für PostgreSQL Server oder Postgre Pro Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

2. Kommunikationsanfragen vom Administrationsserver werden über den UDP-Port 15000 an alle nicht-mobilen verwalteten Geräte gesendet.

   Administrationsagenten innerhalb einer Broadcast-Domäne senden sich gegenseitig Anfragen. Die Daten werden dann an den Administrationsserver gesendet und dazu verwendet, die Grenzen der Broadcast-Domäne zu definieren und Verteilungspunkte automatisch zuzuweisen (sofern diese Option aktiviert ist).

   Wenn der Administrationsserver keinen direkten Zugriff auf die verwalteten Geräte hat, werden keine direkten Kommunikationsanfragen vom Administrationsserver an diese Geräte gesendet.

3. Informationen über das Herunterfahren verwalteter Geräte werden über den UDP-Port 13000 vom Administrationsagenten an den Administrationsserver übermittelt.

4. Der Administrationsserver empfängt Verbindungen von Administrationsagenten und von sekundären Administrationsservern über den TLS-Port 13000.

   Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den Nicht-TLS-Port 14000 annehmen. Kaspersky Security Center Linux unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, es wird jedoch empfohlen, den TLS-Port 13000 zu verwenden.

5. Die verwalteten Geräte (mit Ausnahme von mobilen Geräten) fordern die Aktivierung über den TCP-Port 17000 an. Das ist nicht erforderlich, wenn das Gerät einen eigenen Internetzugang hat, da das Gerät in einem solchen Fall die Daten direkt über das Internet an die Kaspersky-Server sendet.

6. Der Server der Web Console von Kaspersky Security Center sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

   Die Komponente Identitäts- und Zugriffsverwaltung (IAM) verbindet sich über TLS-Port 13299 mit dem Administrationsserver.

   6a. Daten eines Webbrowsers, der auf einem separaten Gerät des Administrators installiert ist, werden über den TLS-Port 8080 an den Server der Web Console von Kaspersky Security Center übermittelt. Der Server der Web Console von Kaspersky Security Center kann entweder auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

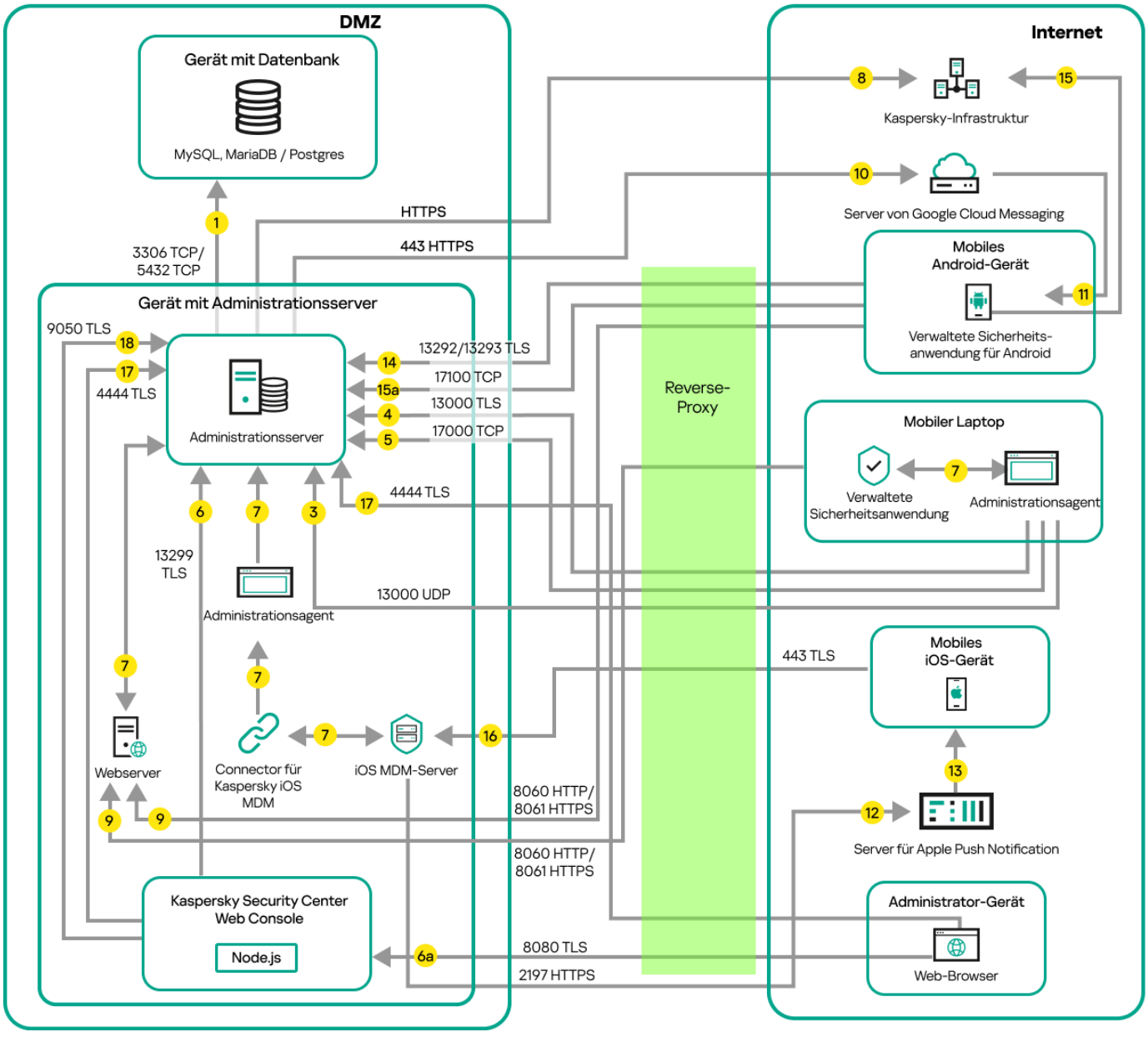
   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

9. Der Server der Kaspersky Security Center Web Console und der Browser (in dem die Kaspersky Security Center Web Console verwendet wird) verbinden sich mit dem Administrationsserver über das OpenID Connect-Authentifizierungsprotokoll durch TLS-Port 4444.

10. Der Server der Kaspersky Security Center Web Console verbindet sich mit dem Administrationsserver über den TLS-Port 9050.

Administrationsserver im LAN, verwaltete Geräte im Internet und Verwendung eines Reverse-Proxys

Die folgende Abbildung zeigt den Datenverkehr für das Szenario, bei dem sich der Administrationsserver im lokalen Netzwerk (LAN) befindet, während sich die verwalteten Geräte im Internet befinden. In dieser Abbildung wird ein beliebiger Reverse-Proxy verwendet. Weitere Einzelheiten entnehmen Sie der Dokumentation dieser Anwendung.



Administrationsserver im lokalen Netzwerk; verwaltete Geräte stellen über einen Reverse-Proxy eine Verbindung zum Administrationsserver her

Dieses Verteilungsschema wird empfohlen, wenn Sie nicht möchten, dass die mobilen Geräte sich direkt mit dem Administrationsserver verbinden, und kein Verbindungs-Gateway in der DMZ zuweisen möchten.

Die Pfeile zeigen die Initiierung des Datenverkehrs an: Jeder Pfeil zeigt von einem Gerät, dass die Verbindung aufbaut, zu dem Gerät, dass auf die Anfrage antwortet. Die Portnummer und der Name des für die Datenübermittlung verwendeten Protokolls sind angegeben. Jeder Pfeil ist mit einer Zahl beschriftet, und für den entsprechenden Datenverkehr gilt:

1. Administrationsserver sendet Daten an die Datenbank. Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server und MariaDB Server oder Port 5432 für PostgreSQL Server oder Postgre Pro Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

2. Kommunikationsanfragen vom Administrationsserver werden über den UDP-Port 15000 an alle nicht-mobilen verwalteten Geräte gesendet.

   Administrationsagenten innerhalb einer Broadcast-Domäne senden sich gegenseitig Anfragen. Die Daten werden dann an den Administrationsserver gesendet und dazu verwendet, die Grenzen der Broadcast-Domäne zu definieren und Verteilungspunkte automatisch zuzuweisen (sofern diese Option aktiviert ist).

   Wenn der Administrationsserver keinen direkten Zugriff auf die verwalteten Geräte hat, werden keine direkten Kommunikationsanfragen vom Administrationsserver an diese Geräte gesendet.

3. Informationen über das Herunterfahren verwalteter Geräte werden über den UDP-Port 13000 vom Administrationsagenten an den Administrationsserver übermittelt.

4. Der Administrationsserver empfängt Verbindungen von Administrationsagenten und von sekundären Administrationsservern über den TLS-Port 13000.

   Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den Nicht-TLS-Port 14000 annehmen. Kaspersky Security Center Linux unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, es wird jedoch empfohlen, den TLS-Port 13000 zu verwenden.

5. Die verwalteten Geräte (mit Ausnahme von mobilen Geräten) fordern die Aktivierung über den TCP-Port 17000 an. Das ist nicht erforderlich, wenn das Gerät einen eigenen Internetzugang hat, da das Gerät in einem solchen Fall die Daten direkt über das Internet an die Kaspersky-Server sendet.

6. Der Server der Web Console von Kaspersky Security Center sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

   Die Komponente Identitäts- und Zugriffsverwaltung (IAM) verbindet sich über TLS-Port 13299 mit dem Administrationsserver.

   6a. Daten eines Webbrowsers, der auf einem separaten Gerät des Administrators installiert ist, werden über den TLS-Port 8080 an den Server der Web Console von Kaspersky Security Center übermittelt. Der Server der Web Console von Kaspersky Security Center kann entweder auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

9. Anfragen für Pakete von verwalteten Geräten, einschließlich mobilen Geräten, werden an den Webserver übermittelt, der sich auf demselben Gerät befindet wie der Administrationsserver.

10. Nur für mobile Android-Geräte: Daten vom Administrationsserver werden an die Google-Server übermittelt. Über diese Verbindung werden mobile Android-Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

11. Nur für mobile Android-Geräte: Push-Benachrichtigungen werden von den Google-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen.

12. Nur für mobile iOS-Geräte: Daten vom iOS MDM-Server werden an die Apple-Server für Push-Benachrichtigungen übermittelt. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

13. Nur für mobile iOS-Geräte: Push-Benachrichtigungen werden von Apple-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile iOS-Geräte darüber benachrichtigt, dass sie eine Verbindung zum iOS MDM-Server herstellen müssen.

14. Nur für mobile Geräte: Die Daten des verwalteten Programms werden über den TLS-Port 13292 / 13293 an den Administrationsserver (oder an das Verbindungs-Gateway) übertragen (entweder direkt oder über einen Reverse-Proxy).

15. Nur für mobile Geräte: Daten vom mobilen Gerät werden an die Infrastruktur von Kaspersky übermittelt.

    Wenn das mobile Gerät über keinen Internetzugang verfügt, werden die Daten an den Administrationsserver über den Port 17100 gesendet, und der Administrationsserver sendet diese anschließend an die Kaspersky-Infrastruktur. Allerdings wird dieses Szenario nur selten verwendet.

16. Nur für mobile iOS-Geräte: Die Daten von mobilen Geräten werden über den TLS-Port 443 an den iOS MDM-Server übermittelt. Dieser befindet sich auf demselben Gerät wie der Administrationsserver oder auf dem Verbindungs-Gateway.

17. Der Server der Kaspersky Security Center Web Console und der Browser (in dem die Kaspersky Security Center Web Console verwendet wird) verbinden sich mit dem Administrationsserver über das OpenID Connect-Authentifizierungsprotokoll durch TLS-Port 4444.

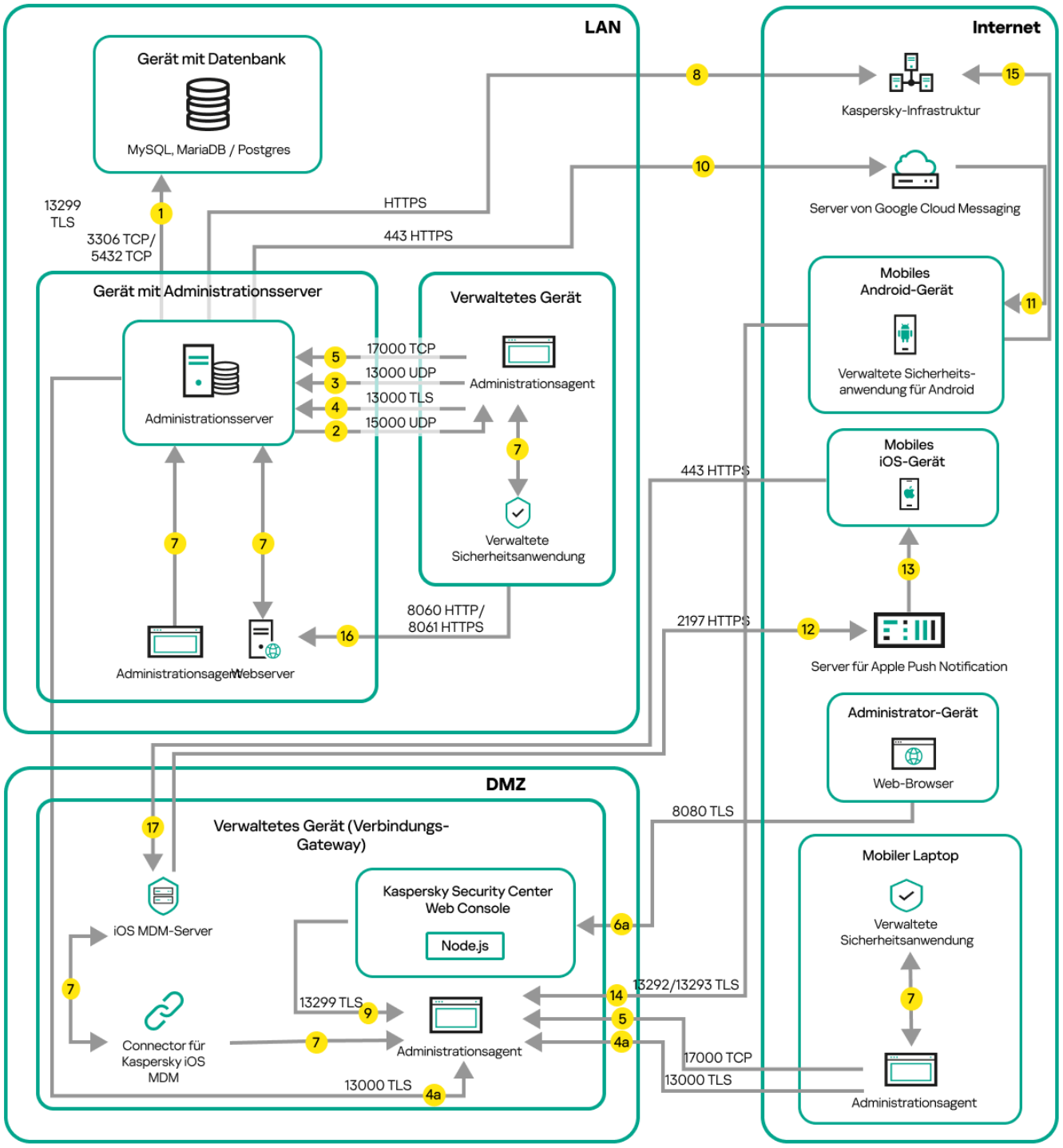
18. Der Server der Kaspersky Security Center Web Console verbindet sich mit dem Administrationsserver über den TLS-Port 9050.

Administrationsserver im LAN, verwaltete Geräte im Internet; Verwendung eines Verbindungs-Gateways

Die folgende Abbildung zeigt den Datenverkehr für das Szenario, bei dem sich der Administrationsserver im lokalen Netzwerk (LAN) befindet, während sich die verwalteten Geräte im Internet befinden. Ein Verbindungs-Gateway wird verwendet.

Dieses Verteilungsschema wird empfohlen, wenn Sie nicht möchten, dass sich die verwalteten Geräte direkt mit dem Administrationsserver verbinden, und weder einen Reverse-Proxy noch eine Unternehmens-Firewall nutzen möchten.

Für dieses Bereitstellungsschema wird die von der Identitäts- und Zugriffsverwaltung (IAM) bereitgestellte Domänenauthentifizierung (Single Sign-On) nicht unterstützt.



Verwaltete mobile Geräte, die über ein Verbindungs-Gateway mit dem Administrationsserver verbunden sind

In dieser Abbildung sind die verwalteten Geräte über ein Verbindungs-Gateway, welches sich in der DMZ befindet, mit dem Administrationsserver verbunden. Es wird kein Reverse-Proxy und keine Unternehmens-Firewall verwendet.

Die Pfeile zeigen die Initiierung des Datenverkehrs an: Jeder Pfeil zeigt von einem Gerät, dass die Verbindung aufbaut, zu dem Gerät, d1ass auf die Anfrage antwortet. Die Portnummer und der Name des für die Datenübermittlung verwendeten Protokolls sind angegeben. Jeder Pfeil ist mit einer Zahl beschriftet, und für den entsprechenden Datenverkehr gilt:

1. Administrationsserver sendet Daten an die Datenbank. Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server und MariaDB Server oder Port 5432 für PostgreSQL Server oder Postgre Pro Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

2. Kommunikationsanfragen vom Administrationsserver werden über den UDP-Port 15000 an alle nicht-mobilen verwalteten Geräte gesendet.

   Administrationsagenten innerhalb einer Broadcast-Domäne senden sich gegenseitig Anfragen. Die Daten werden dann an den Administrationsserver gesendet und dazu verwendet, die Grenzen der Broadcast-Domäne zu definieren und Verteilungspunkte automatisch zuzuweisen (sofern diese Option aktiviert ist).

   Wenn der Administrationsserver keinen direkten Zugriff auf die verwalteten Geräte hat, werden keine direkten Kommunikationsanfragen vom Administrationsserver an diese Geräte gesendet.

3. Informationen über das Herunterfahren verwalteter Geräte werden über den UDP-Port 13000 vom Administrationsagenten an den Administrationsserver übermittelt.

4. Der Administrationsserver empfängt Verbindungen von Administrationsagenten und von sekundären Administrationsservern über den TLS-Port 13000.

   Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den Nicht-TLS-Port 14000 annehmen. Kaspersky Security Center Linux unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, es wird jedoch empfohlen, den TLS-Port 13000 zu verwenden.

   4a. Ein in der DMZ vorhandenes Verbindungs-Gateway empfängt ebenfalls Verbindungen vom Administrationsserver über den TLS-Port 13000. Da ein Verbindungs-Gateway innerhalb der demilitarisierten Zone die Ports des Administrationsservers nicht erreichen kann, etabliert und erhält der Administrationsserver eine permanente Signalverbindung mit einem Verbindungs-Gateway. Die Signalverbindung wird nicht zum Datentransfer verwendet, sondern lediglich, um eine Einladung zur Netzwerk-Interaktion zu übertragen. Wenn ein Verbindungs-Gateway eine Verbindung zum Administrationsserver benötigt, informiert das Gateway den Server mittels der Signalverbindung darüber und anschließend stellt der Server die benötigte Verbindung für den Datentransfer her.

   Mobile Geräte verbinden sich mit dem Verbindungs-Gateway ebenfalls über den TLS-Port 13000.

5. Die verwalteten Geräte (mit Ausnahme von mobilen Geräten) fordern die Aktivierung über den TCP-Port 17000 an. Das ist nicht erforderlich, wenn das Gerät einen eigenen Internetzugang hat, da das Gerät in einem solchen Fall die Daten direkt über das Internet an die Kaspersky-Server sendet.

6. Der Server der Web Console von Kaspersky Security Center sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

   6a. Daten eines Webbrowsers, der auf einem separaten Gerät des Administrators installiert ist, werden über den TLS-Port 8080 an den Server der Web Console von Kaspersky Security Center übermittelt. Der Server der Web Console von Kaspersky Security Center kann entweder auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

9. Anfragen für Pakete von verwalteten Geräten, einschließlich mobilen Geräten, werden an den Webserver übermittelt, der sich auf demselben Gerät befindet wie der Administrationsserver.

10. Nur für mobile Android-Geräte: Daten vom Administrationsserver werden an die Google-Server übermittelt. Über diese Verbindung werden mobile Android-Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

11. Nur für mobile Android-Geräte: Push-Benachrichtigungen werden von den Google-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen.

12. Nur für mobile iOS-Geräte: Daten vom iOS MDM-Server werden an die Apple-Server für Push-Benachrichtigungen übermittelt. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

13. Nur für mobile iOS-Geräte: Push-Benachrichtigungen werden von Apple-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile iOS-Geräte darüber benachrichtigt, dass sie eine Verbindung zum iOS MDM-Server herstellen müssen.

14. Nur für mobile Geräte: Die Daten des verwalteten Programms werden über den TLS-Port 13292 / 13293 an den Administrationsserver (oder an das Verbindungs-Gateway) übertragen (entweder direkt oder über einen Reverse-Proxy).

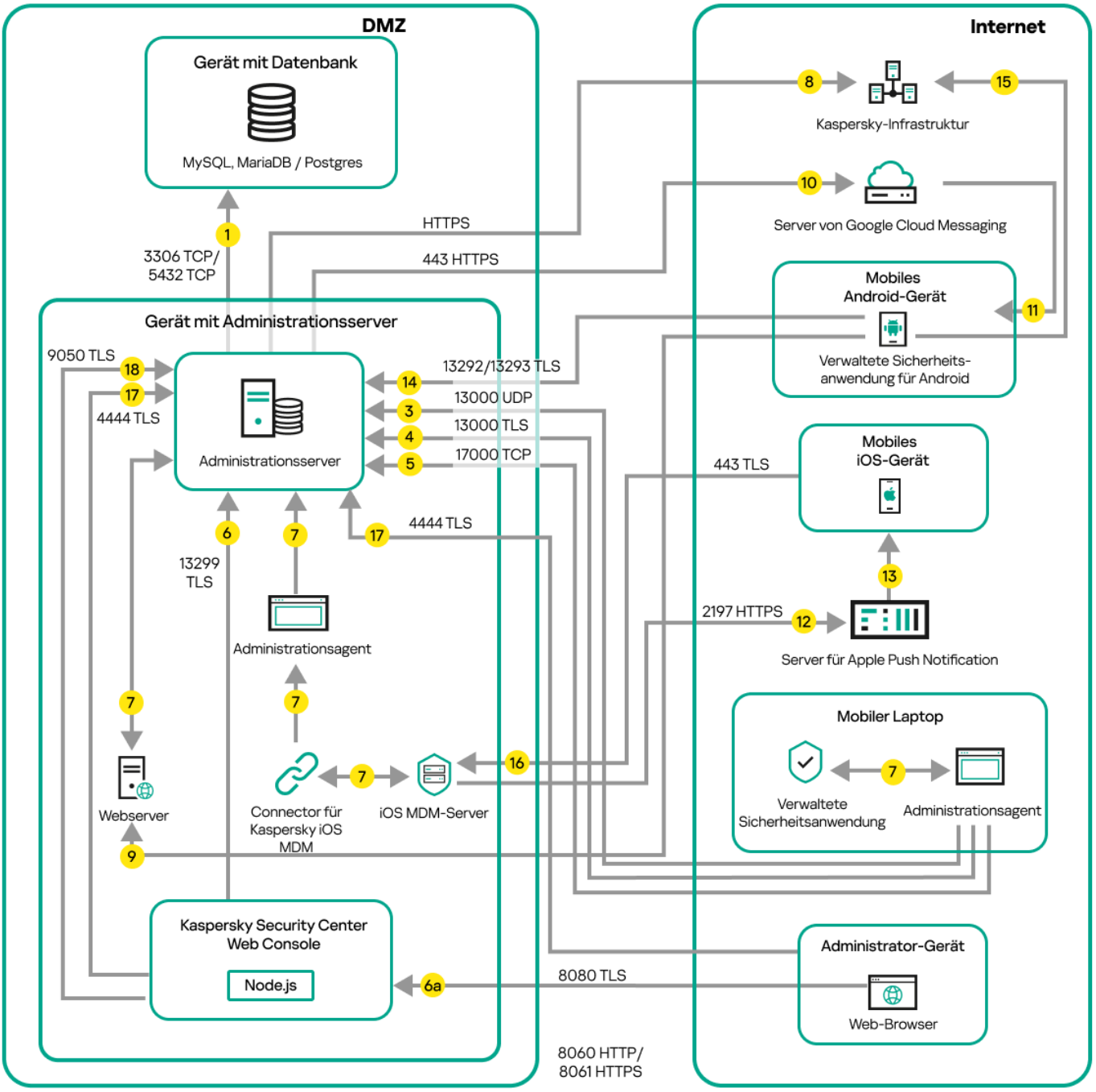
15. Nur für mobile Geräte: Daten vom mobilen Gerät werden an die Infrastruktur von Kaspersky übermittelt.

    Wenn das mobile Gerät über keinen Internetzugang verfügt, werden die Daten an den Administrationsserver über den Port 17100 gesendet, und der Administrationsserver sendet diese anschließend an die Kaspersky-Infrastruktur. Allerdings wird dieses Szenario nur selten verwendet.

16. Nur für mobile iOS-Geräte: Die Daten von mobilen Geräten werden über den TLS-Port 443 an den iOS MDM-Server übermittelt. Dieser befindet sich auf demselben Gerät wie der Administrationsserver oder auf dem Verbindungs-Gateway.

Administrationsserver in der DMZ, verwaltete Geräte im Internet

Die folgende Abbildung zeigt den Datenverkehr für das Szenario, bei dem sich der Administrationsserver in der demilitarisierten Zone (DMZ) befindet, während sich die verwalteten Geräte im Internet befinden.



Administrationsserver in der DMZ, verwaltete mobile Geräte im Internet

In dieser Abbildung wird kein Verbindungs-Gateway verwendet: Die mobilen Geräte stellen eine Direktverbindung zum Administrationsserver her.

Die Pfeile zeigen die Initiierung des Datenverkehrs an: Jeder Pfeil zeigt von einem Gerät, dass die Verbindung aufbaut, zu dem Gerät, d1ass auf die Anfrage antwortet. Die Portnummer und der Name des für die Datenübermittlung verwendeten Protokolls sind angegeben. Jeder Pfeil ist mit einer Zahl beschriftet, und für den entsprechenden Datenverkehr gilt:

1. Administrationsserver sendet Daten an die Datenbank. Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät bereitstellen, auf dem sich die Datenbank befindet (zum Beispiel: Port 3306 für MySQL Server und MariaDB Server oder Port 5432 für PostgreSQL Server oder Postgre Pro Server). Relevante Informationen finden Sie in der DBMS-Dokumentation.

2. Kommunikationsanfragen vom Administrationsserver werden über den UDP-Port 15000 an alle nicht-mobilen verwalteten Geräte gesendet.

   Administrationsagenten innerhalb einer Broadcast-Domäne senden sich gegenseitig Anfragen. Die Daten werden dann an den Administrationsserver gesendet und dazu verwendet, die Grenzen der Broadcast-Domäne zu definieren und Verteilungspunkte automatisch zuzuweisen (sofern diese Option aktiviert ist).

   Wenn der Administrationsserver keinen direkten Zugriff auf die verwalteten Geräte hat, werden keine direkten Kommunikationsanfragen vom Administrationsserver an diese Geräte gesendet.

3. Informationen über das Herunterfahren verwalteter Geräte werden über den UDP-Port 13000 vom Administrationsagenten an den Administrationsserver übermittelt.

4. Der Administrationsserver empfängt Verbindungen von Administrationsagenten und von sekundären Administrationsservern über den TLS-Port 13000.

   Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den Nicht-TLS-Port 14000 annehmen. Kaspersky Security Center Linux unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, es wird jedoch empfohlen, den TLS-Port 13000 zu verwenden.

5. Die verwalteten Geräte (mit Ausnahme von mobilen Geräten) fordern die Aktivierung über den TCP-Port 17000 an. Das ist nicht erforderlich, wenn das Gerät einen eigenen Internetzugang hat, da das Gerät in einem solchen Fall die Daten direkt über das Internet an die Kaspersky-Server sendet.

6. Der Server der Web Console von Kaspersky Security Center sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

   Die Komponente Identitäts- und Zugriffsverwaltung (IAM) verbindet sich über TLS-Port 13299 mit dem Administrationsserver.

   6a. Daten eines Webbrowsers, der auf einem separaten Gerät des Administrators installiert ist, werden über den TLS-Port 8080 an den Server der Web Console von Kaspersky Security Center übermittelt. Der Server der Web Console von Kaspersky Security Center kann entweder auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

9. Anfragen für Pakete von verwalteten Geräten werden an den Webserver übermittelt, der sich auf demselben Gerät befindet wie der Administrationsserver.

10. Nur für mobile Android-Geräte: Daten vom Administrationsserver werden an die Google-Server übermittelt. Über diese Verbindung werden mobile Android-Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet. Der FCM-Dienst wird auch auf HTTPS-Port 443 ausgeführt.

11. Nur für mobile Android-Geräte: Push-Benachrichtigungen werden von den Google-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile Geräte darüber benachrichtigt, dass sie eine Verbindung zum Administrationsserver herstellen müssen.

12. Nur für mobile iOS-Geräte: Daten vom iOS MDM-Server werden an die Apple-Server für Push-Benachrichtigungen übermittelt. Anschließend werden Push-Benachrichtigungen an die mobilen Geräte gesendet.

13. Nur für mobile iOS-Geräte: Push-Benachrichtigungen werden von Apple-Servern an das mobile Gerät gesendet. Über diese Verbindung werden mobile iOS-Geräte darüber benachrichtigt, dass sie eine Verbindung zum iOS MDM-Server herstellen müssen.

14. Nur für mobile Geräte: Die Daten des verwalteten Programms werden über den TLS-Port 13292 / 13293 an den Administrationsserver (oder an das Verbindungs-Gateway) übertragen (entweder direkt oder über einen Reverse-Proxy).

15. Nur für mobile Geräte: Daten vom mobilen Gerät werden an die Infrastruktur von Kaspersky übermittelt.

    Wenn das mobile Gerät über keinen Internetzugang verfügt, werden die Daten an den Administrationsserver über den Port 17100 gesendet, und der Administrationsserver sendet diese anschließend an die Kaspersky-Infrastruktur. Allerdings wird dieses Szenario nur selten verwendet.

16. Nur für mobile iOS-Geräte: Die Daten von mobilen Geräten werden über den TLS-Port 443 an den iOS MDM-Server übermittelt. Dieser befindet sich auf demselben Gerät wie der Administrationsserver oder auf dem Verbindungs-Gateway.

17. Der Server der Kaspersky Security Center Web Console und der Browser (in dem die Kaspersky Security Center Web Console verwendet wird) verbinden sich mit dem Administrationsserver über das OpenID Connect-Authentifizierungsprotokoll durch TLS-Port 4444.

18. Der Server der Kaspersky Security Center Web Console verbindet sich mit dem Administrationsserver über den TLS-Port 9050.

Interaktion der Komponenten von Kaspersky Security Center Linux und der Sicherheitsanwendungen: weitere Informationen

Dieser Abschnitt enthält die Interaktionsschemata zwischen den Komponenten von Kaspersky Security Center Linux und den verwalteten Sicherheitsanwendungen. In den Schemata sind die Portnummern, die geöffnet sein müssen, sowie die Namen der Prozesse, mit denen die Ports geöffnet werden, angeführt.

Konventionen für die Interaktionsschemata

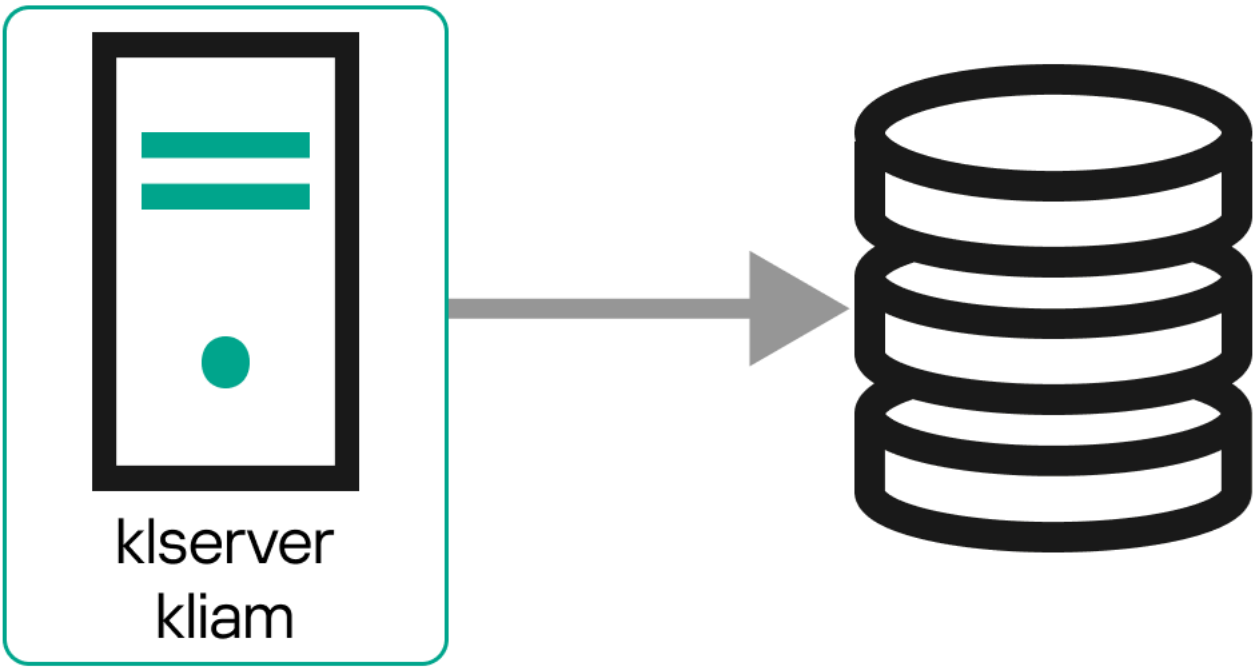
In der nachfolgenden Tabelle sind die festgelegten Bezeichnungen angeführt, die in den Schemas verwendet werden.

Formatierung mit besonderer Bedeutung

Zeichen	Erklärung
	Administrationsserver
	Sekundärer Administrationsserver
	DBMS
	Client-Gerät, auf dem der Administrationsagent und ein Programm der Reihe Kaspersky Endpoint Security (oder einer anderen Sicherheitsanwendung, die von Kaspersky Security Center Linux verwaltet werden kann) installiert sind
	Verbindungs-Gateway
	Verteilungspunkt
	Browser auf dem Gerät des Benutzers
	Prozess, der auf dem Gerät gestartet wird und bestimmte Ports öffnet
	Port und Nummer
	TCP-Datenverkehr (die Pfeilrichtung bezeichnet die Richtung des Verkehrs)
	UDP-Datenverkehr (die Pfeilrichtung bezeichnet die Richtung des Verkehrs)
	DBMS-Transport
	Grenze der demilitarisierten Zone

Administrationsserver und DBMS

Die Daten des Administrationsservers und der Identitäts- und Zugriffsverwaltung (IAM) werden in separaten Datenbanken innerhalb desselben DBMS gespeichert.



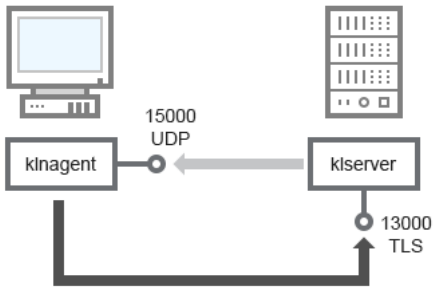
Administrationsserver, Identitäts- und Zugriffsverwaltung und DBMS

Wenn Sie den Administrationsserver und die Datenbank auf unterschiedlichen Geräten installieren, müssen Sie die erforderlichen Ports auf dem Gerät, auf dem sich die Datenbank befindet, bereitstellen (zum Beispiel: Port 3306 für MariaDB). Die entsprechenden Informationen finden Sie in der DBMS-Dokumentation.
Der Port für die Verbindung von IAM mit dem DBMS wird vom Benutzer während der Installation von Kaspersky Security Center Linux angegeben.

Wenn der Administrationsserver auf ein anderes Gerät verschoben oder deinstalliert wird, löscht der Server weder seine Datenbank noch die IAM-Datenbank automatisch. Bei Bedarf müssen Sie die Datenbanken selbstständig entfernen.

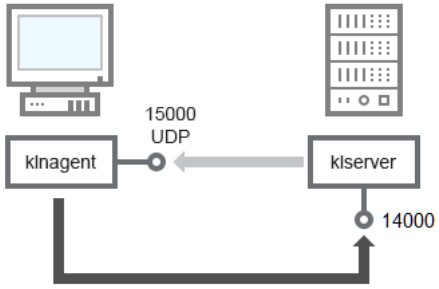
Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendung

Der Administrationsserver nimmt die Verbindungen der Administrationsagenten über TLS-Port 13000 (SSL) an (s. Abb. unten).



Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendungen, Verbindung über Port 13000 (empfohlen)

Wenn Sie eine der Vorgängerversionen von Kaspersky Security Center Linux verwendet haben, kann der Administrationsserver in Ihrem Netzwerk Verbindungen von Administrationsagenten über den ungeschützten Port 14000 (kein SSL) annehmen (s. Abb. unten). Kaspersky Security Center Linux unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den SSL-Port 13000 zu verwenden.



Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendungen, Verbindung über Port 14000 (niedrigere Sicherheit)

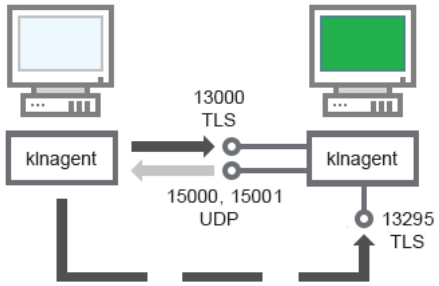
Erklärungen zum Schema finden Sie in den nachfolgenden Tabellen.

Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendung (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports
Administrationsagent	15000	klnagent	UDP	Multicast an die Administrationsagenten
Administrationsserver	13000	klserver	TCP (TLS)	Annahme der Verbindungen von den Administrationsagenten
Administrationsserver	14000	klserver	TCP	Annahme der Verbindungen von den Administrationsagenten

Software-Upgrades auf dem Client-Gerät mithilfe des Verteilungspunkts

Das Client-Gerät stellt eine Verbindung zum Verteilungspunkt über den Port 13000 und, falls Sie den Verteilungspunkt als Push-Server verwenden, über den Port 13295 her; der Verteilungspunkt verwendet Port 15000 für Multicast an die Administrationsagenten (s. Abb. unten). Updates und Installationspakete werden von einem Verteilungspunkt über Port 15001 empfangen.



Software-Update auf dem Client-Gerät über einen Verteilungspunkt

Erklärungen zum Schema finden Sie in der unteren Tabelle.

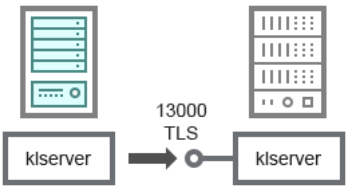
Software-Update über einen Verteilungspunkt (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports
Administrationsagent	15000	klnagent	UDP	Multicast an die Administrationsagenten
Administrationsagent	15001	klnagent	UDP	Empfang von Updates und Installationspaketen von einem Verteilungspunkt
Verteilungspunkt	13000	klnagent	TCP (TLS)	Annahme der Verbindungen von den Administrationsagenten
Verteilungspunkt	13295	klnagent	TCP (TLS)	Annehmen der Verbindungen von Client-Geräten (Server-Push)

Hierarchie der Administrationsserver: primärer Administrationsserver und sekundärer Administrationsserver

Das Schema (s. Abb. unten) zeigt, wie der Port 13000 für die Interaktion der Administrationsserver, die in der Hierarchie zusammengefasst sind, verwendet wird.

Im Weiteren können Sie nach der Zusammenfassung der Server und der Hierarchie beide Server über die Kaspersky Security Center Web Console verwalten, die mit dem primären Administrationsserver verbunden ist. Auf diese Weise muss nur der Port 13299 des primären Administrationsservers verfügbar sein.



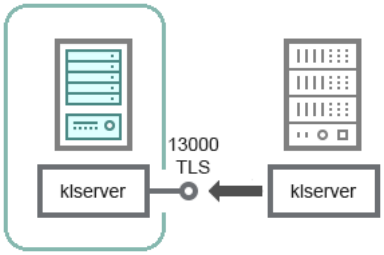
Hierarchie der Administrationsserver: primärer Administrationsserver und sekundärer Administrationsserver

Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

Administrationsserver-Hierarchie (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports
Primärer Administrationsserver	13000	klserver	TCP (TLS)	Empfangen von Verbindungen von sekundären Administrationsservern

Hierarchie der Administrationsserver mit sekundärem Administrationsserver in der demilitarisierten Zone



Hierarchie der Administrationsserver mit sekundärem Administrationsserver in der demilitarisierten Zone

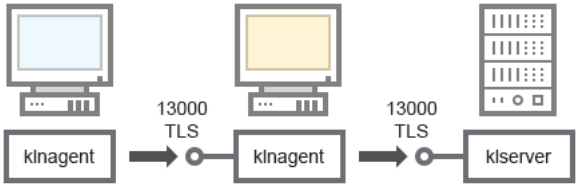
Das Schema zeigt die Hierarchie der Administrationsserver, in welcher der sekundäre Administrationsserver, der sich in der demilitarisierten Zone befindet, die Verbindung vom primären Administrationsserver übernimmt (eine Erklärung zum Schema finden Sie in der nachstehenden Tabelle). Bei der Zusammenfassung der Administrationsserver in der Hierarchie ist es erforderlich, dass der Port 13299 beider Server verfügbar ist. Die Kaspersky Security Center Web Console verbindet sich mit dem Administrationsserver über den SSL-Port TCP 13299.

Im Weiteren können Sie nach der Zusammenfassung der Server und der Hierarchie beide Server über die Kaspersky Security Center Web Console verwalten, die mit dem primären Administrationsserver verbunden ist. Auf diese Weise muss nur der Port 13299 des primären Administrationsservers verfügbar sein.

Hierarchie der Administrationsserver mit einem sekundären Administrationsserver in der demilitarisierten Zone (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports
Sekundärer Administrationsserver	13000	klserver	TCP (TLS)	Aufnahme der Verbindungen vom primären Administrationsserver

Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät



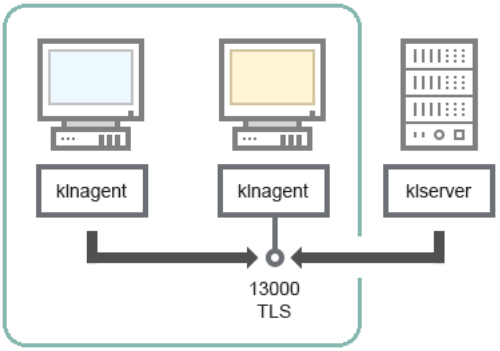
Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät

Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports
Administrationsserver	13000	klserver	TCP (TLS)	Annahme der Verbindungen von den Administrationsagenten
Administrationsagent	13000	klnagent	TCP (TLS)	Annahme der Verbindungen von den Administrationsagenten

Administrationsserver und zwei Geräte in der DMZ: ein Verbindungs-Gateway und ein Client-Gerät



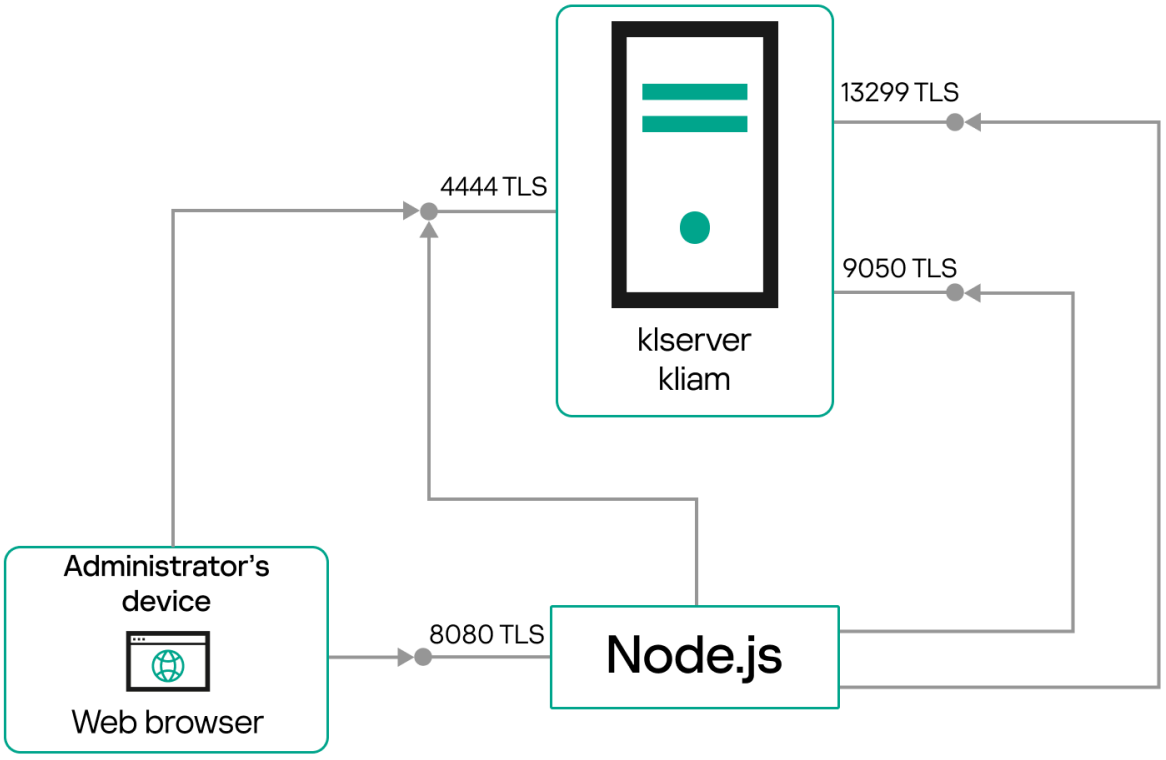
Administrationsserver Verbindungs-Gateway und Client-Gerät in der demilitarisierten Zone

Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports
Administrationsagent	13000	klnagent	TCP (TLS)	Annahme der Verbindungen von den Administrationsagenten

Administrationsserver und Kaspersky Security Center Web Console



Administrationsserver und Kaspersky Security Center Web Console

Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

Administrationsserver und Kaspersky Security Center Web Console (Datenverkehr)

Gerät	Portnummer	Name des Prozesses, der den Port öffnet	Protokoll	Zweck des Ports
Administrationsserver	13299	klserver	TCP (TLS)	Empfangen von Verbindungen von der Kaspersky Security Center Web Console und der Identitäts- und Zugriffsverwaltung (IAM) zum Administrationsserver über OpenAPI.
Server der Web Console von Kaspersky Security Center oder Administrationsserver	8080	Node.js: Serverseitiges JavaScript	TCP (TLS)	Empfangen von Verbindungen von Kaspersky Security Center Web Console
Administrationsserver	4444	kliam	TCP (TLS)	Empfangen von Verbindungen vom Server der Kaspersky Security Center Web Console und dem Browser (in dem Kaspersky Security Center Web Console verwendet wird) zum Administrationsserver mit IAM über das OpenID Connect-Authentifizierungsprotokoll.
Administrationsserver	9050	kliam	TCP (TLS)	Empfangen von Verbindungen von Kaspersky Security Center Web Console zu IAM

Die Kaspersky Security Center Web Console kann auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

Erste Schritte

Nach diesem Szenario können Sie den Kaspersky Security Center Linux Administrationsserver und Kaspersky Security Center Web Console installieren, mithilfe des Schnellstartassistenten die Ersteinrichtung des Administrationsservers durchführen und mithilfe des Assistenten für die Bereitstellung des Schutzes Kaspersky-Anwendungen auf den verwalteten Geräten installieren.

Erforderliche Vorrausetzungen

Sie müssen einen Lizenzschlüssel (Aktivierungscode) für Kaspersky Endpoint Security for Business oder Lizenzschlüssel (Aktivierungscodes) für Kaspersky-Sicherheitsanwendungen haben.

Wenn Sie Kaspersky Security Center Linux zuerst ausprobieren möchten, können Sie von der Kaspersky-Website eine kostenlose 30-Tage-Testversion herunterladen.

Schritte

Das Hauptinstallationsszenario besteht aus den folgenden Schritten:

1. **Struktur des Schutzes in der Organisation auswählen**

   Erfahren Sie mehr über die Komponenten von Kaspersky Security Center Linux. Bestimmen Sie ausgehend von der Konfiguration des Netzwerks und der Bandbreite der Übertragungskanäle, wie viele Administrationsserver verwendet und wie sie über Ihre Büros verteilt werden sollen (sofern Sie ein verteiltes Netzwerk verwenden).

   Legen Sie fest, ob eine Hierarchie der Administrationsserver in der Organisation verwendet werden soll. Dazu müssen Sie ermitteln, ob es möglich und sinnvoll ist, alle Client-Geräte mit einem einzigen Administrationsserver zu verwalten, oder ob eine Hierarchie der Administrationsserver aufgebaut werden sollte. Möglicherweise müssen Sie auch eine Hierarchie der Administrationsserver aufbauen, die mit der Organisationsstruktur des Unternehmens übereinstimmt, dessen Netzwerk Sie schützen möchten.

2. **Vorbereitung der Verwendung benutzerdefinierter Zertifikate**

   Wenn die Public-Key-Infrastruktur (PKI) in Ihrer Organisation die Verwendung von benutzerdefinierten, von einer bestimmten Zertifizierungsstelle (Certification Authority - CA) ausgestellten, Zertifikaten erfordert, bereiten Sie diese Zertifikate vor und stellen Sie sicher, dass sie alle Voraussetzungen erfüllen.

3. **Installation eines Datenbank-Managementsystems (DBMS)**

   Installation des DBMS oder eines anderen Systems, das von Kaspersky Security Center Linux verwendet werden soll.

   Sie können eine der unterstützten DBMS auswählen. Informationen zur Installation des ausgewählten DBMS finden Sie in dessen Dokumentation.

   Wenn die Distribution Ihres Linux-basierten Betriebssystems ohne unterstütztes DBMS ausgeliefert wird, können Sie das DBMS aus der Paketverwaltung eines Drittanbieters installieren. Wenn die Installation von Software aus Drittanbieter-Paketverwaltungen untersagt ist, können Sie das DBMS auf einem separaten Gerät installieren.

   > Wenn Sie sich entscheiden, PostgreSQL oder Postgres Pro als DBMS zu installieren, stellen Sie sicher, dass Sie ein Kennwort für den Superuser angegeben haben. Wenn das Kennwort nicht angegeben wird, kann sich der Administrationsserver möglicherweise nicht mit der Datenbank verbinden.

Wenn Sie MariaDB, PostgreSQL, oder Postgres Pro installieren, verwenden Sie die empfohlenen Einstellungen, um sicherzustellen, dass das DBMS ordnungsgemäß funktioniert.

Wenn Sie den DBMS-Typ nach der Installation ändern möchten, müssen Sie Kaspersky Security Center Linux erneut installieren. Sie können Aufgaben und Richtlinien exportieren, um sie nach der Neuinstallation wieder zu importieren. Weitere Informationen dazu finden Sie in den folgenden Artikeln: Aufgaben exportieren und Richtlinien exportieren.

4. **Konfiguration der Ports**

   Stellen Sie sicher, dass die Ports geöffnet sind, die für die Interaktion der Komponenten entsprechend der von Ihnen ausgewählten Schutzstruktur benötigt werden.

   Wenn der Zugriff auf den Administrationsserver über das Internet gewährt werden muss, konfigurieren Sie die Ports und die Verbindungseinstellungen je nach Netzwerkkonfiguration.

5. **Kaspersky Security Center Linux installieren**

   Wählen Sie ein Linux-Gerät aus, das Sie als Administrationsserver verwenden möchten, stellen Sie sicher, dass das Gerät die Software- und Hardwareanforderungen erfüllt, und installieren Sie dann Kaspersky Security Center Linux auf dem Gerät. Die Serverversion des Administrationsagenten wird zusammen mit dem Administrationsserver installiert.

6. **Kaspersky Security Center Web Console und Verwaltungs-Web-Plug-ins installieren**

   Wählen Sie ein Linux-Gerät aus, das Sie als Administrator-Arbeitsplatz verwenden möchten, stellen Sie sicher, dass das Gerät die Software- und Hardwareanforderungen erfüllt, und installieren Sie dann Kaspersky Security Center Web Console auf dem Gerät. Sie können Kaspersky Security Center Web Console entweder auf demselben Gerät installieren, auf dem der Administrationsserver installiert ist, oder auf einem anderen Gerät.

   Laden Sie das Verwaltungs-Web-Plug-in für Kaspersky Endpoint Security für Linux herunter und installieren Sie es dann auf demselben Gerät, auf dem Kaspersky Security Center Web Console installiert ist.

7. **Kaspersky Endpoint Security für Linux und den Administrationsagenten auf dem Gerät mit dem Administrationsserver installieren**

   Standardmäßig betrachtet die Anwendung das Gerät mit dem Administrationsserver nicht als verwaltetes Gerät. Um den Administrationsserver vor Viren und anderen Bedrohungen zu schützen und das Gerät wie alle anderen verwalteten Geräte zu verwalten, empfehlen wir Ihnen, Kaspersky Endpoint Security für Linux und den Administrationsagenten für Linux auf dem Gerät des Administrationsservers zu installieren. In diesem Fall wird der Administrationsagent für Linux installiert und funktioniert unabhängig von der Serverversion des Administrationsagenten, die Sie zusammen mit dem Administrationsserver installiert haben.

8. **Erstkonfiguration vornehmen**

   Nach Abschluss der Installation des Administrationsservers wird bei der ersten Verbindung mit dem Administrationsserver automatisch der Schnellstartassistent ausgeführt. Befolgen Sie die Schritte des Assistenten, um die Erstkonfiguration des Administrationsservers nach Bedarf vorzunehmen. Während der Erstkonfiguration erstellt der Assistent die zur Bereitstellung des Schutzes notwendigen Richtlinien und Aufgaben mit Standardeinstellungen. Diese Einstellungen sind eventuell nicht optimal für Ihr Unternehmen geeignet. Sie können bei Bedarf die Einstellungen der Richtlinien und Aufgaben ändern.

9. **Suche der Geräte im Netzwerk**

   Ermitteln Sie die Geräte manuell. Daraufhin erhält Kaspersky Security Center Linux die Adressen und die Namen aller Geräte, die im Netzwerk registriert sind. Anschließend können Sie Kaspersky Security Center Linux verwenden, um Kaspersky-Anwendungen und Software von anderen Herstellern auf den gefundenen Geräten zu installieren. Da Kaspersky Security Center Linux die Gerätesuche regelmäßig startet, werden neue Geräte im Netzwerk automatisch gefunden, sobald sie auftauchen.

10. **Geräte in Administrationsgruppen anordnen**

    In einigen Fällen müssen für die optimale Implementierung des Schutzes auf den Geräten im Netzwerk die Geräte unter Berücksichtigung der Organisationsstruktur des Unternehmens in Administrationsgruppen zusammengefasst werden. Sie können Verschiebungsregeln für die Verteilung der Geräte auf Gruppen erstellen oder die Geräte manuell verteilen. Für Administrationsgruppen können Gruppenaufgaben und Gültigkeitsbereiche von Richtlinien bestimmt und Verteilungspunkte zugewiesen werden.

    Stellen Sie sicher, dass alle verwalteten Geräte den entsprechenden Administrationsgruppen zugewiesen wurden und dass keine nicht zugeordneten Geräte mehr im Netzwerk vorhanden sind.

11. **Verteilungspunkte zuweisen**

    Verteilungspunkte werden den Administrationsgruppen automatisch zugewiesen, bei Bedarf können Sie diese aber auch manuell zuweisen. In den folgenden Fällen wird die Verwendung von Verteilungspunkten empfohlen: in großen Netzwerken, um die Auslastung des Administrationsservers zu senken, sowie in Netzwerken mit einer verteilten Struktur, um dem Administrationsserver Zugriff auf Geräte oder Gerätegruppen zu gewähren, die über Kanäle mit geringer Bandbreite verbunden sind.

12. **Installation des Administrationsagenten und der Sicherheitsanwendungen auf den Geräten im Netzwerk**

    Als Bereitstellung des Schutzes in einem Unternehmensnetzwerk wird die Installation von Administrationsagenten und Sicherheitsanwendungen auf den Geräten verstanden, die vom Administrationsserver bei der Gerätesuche im Unternehmensnetzwerk gefunden wurden.

    Um die Anwendungen remote zu installieren, führen Sie den Assistenten für die Bereitstellung des Schutzes aus.

    Die Sicherheitsanwendungen schützen Geräte vor Viren und anderen Anwendungen, die eine Bedrohung darstellen. Der Administrationsagent gewährleistet die Verbindung des Geräts mit dem Administrationsserver. Die Einstellungen des Administrationsagenten werden standardmäßig automatisch angepasst.

    Bevor Sie den Administrationsagenten und die Sicherheitsanwendung auf Geräten im Netzwerk installieren, stellen Sie sicher, dass diese Geräte verfügbar (aktiviert) sind.

13. **Lizenzschlüssel auf Client-Geräte verteilen**

    Verteilen Sie die Lizenzschlüssel auf die Client-Geräte, um die verwalteten Sicherheitsanwendungen auf diesen Geräten zu aktivieren.

14. **Konfigurieren von Richtlinien für Kaspersky-Anwendungen**

    Um verschiedene Anwendungseinstellungen auf verschiedene Geräte anzuwenden, können Sie eine geräteorientierte Sicherheitsverwaltung und/oder eine benutzerorientierte Sicherheitsverwaltung verwenden. Die geräteorientierte Sicherheitsverwaltung kann über Richtlinien und Aufgaben implementiert werden. Sie können Aufgaben nur auf die Geräte anwenden, die bestimmte Bedingungen erfüllen. Um Bedingungen für das Filtern von Geräten festzulegen, verwenden Sie die Geräteauswahl und Tags.

15. **Überwachen des Netzwerkschutzstatus**

    Sie können Ihr Netzwerk mithilfe von Widgets auf dem Dashboard überwachen, Berichte in Kaspersky-Anwendungen erstellen sowie von Anwendungen auf verwalteten Geräten empfangene Ereignisauswahlen und Benachrichtigungslisten anzeigen.

Härtungsleitfaden

Kaspersky Security Center Linux dient dazu, die wichtigsten Aufgaben zur Verwaltung und Wartung des Antiviren-Schutzes in einem Unternehmensnetzwerk zentral zu erledigen. Das Programm bietet dem Administrator Zugriff auf detaillierte Informationen über die Qualität der Netzwerksicherheit der Organisation. Mit Kaspersky Security Center Linux können Sie alle Schutzkomponenten konfigurieren, die mithilfe von Kaspersky-Anwendungen erstellt wurden.

Der Kaspersky Security Center Linux Administrationsserver hat vollen Zugriff auf die Schutzverwaltung der Client-Geräte und ist die wichtigste Komponente des Sicherheitssystems der Organisation. Daher sind für den Administrationsserver erhöhte Schutzmaßnahmen erforderlich.

Erstellen Sie vor der Konfiguration eine Backup-Kopie des Kaspersky Security Center Linux Administrationsservers mithilfe der Aufgabe Backup der Daten des Administrationsservers anlegen oder des Tools "klbackup" und speichern Sie diese an einem sicheren Ort.

Der Härtungsleitfaden beschreibt Empfehlungen und Funktionen zur Konfiguration von Kaspersky Security Center Linux und seinen Komponenten, mit dem Ziel, das Risiko einer Kompromittierung zu verringern.

Der Härtungsleitfaden enthält die folgenden Informationen:

- Auswahl der Administrationsserver-Architektur
- Konfigurieren einer sicheren Verbindung zum Administrationsserver
- Konfigurieren der Benutzerkonten, um auf den Administrationsserver zuzugreifen
- Verwaltung des Schutzes des Administrationsservers
- Verwaltung des Schutzes der Client-Geräte
- Konfigurieren des Schutzes für verwaltete Programme
- Wartung des Administrationsservers
- Übertragen von Informationen an Drittanbieter-Anwendungen
- Sicherheitsempfehlungen für Drittanbieter-Informationssysteme

Checkliste zur Härtung

Bereitstellung des Administrationsservers

- Installieren Sie den Administrationsserver auf einem dedizierten physischen oder virtuellen Server.
- Verwenden Sie den dedizierten Server nicht, um andere Dienste auszuführen.
- Installieren Sie den Administrationsserver (im Weiteren auch "Server" genannt) nicht auf einem:
  - Domänencontroller
  - Terminalserver
  - Benutzergerät

Verbindungssicherheit

- Konfigurieren Sie eine Firewall, um den Zugriff auf das Gerät des Servers über alle Ports und Protokolle, mit Ausnahme der vom Server benötigten Ports, einzuschränken. Erlauben Sie den Zugriff auf das Gerät des Servers nur von vertrauenswürdigen Geräten.
- Konfigurieren Sie eine Allow-Liste mit IP-Adressen für die Server-Ports, die zur Verbindung der Kaspersky Security Center Web Console (im Weiteren auch "Web Console" genannt) mit dem Server verwendet werden.
- Konfigurieren Sie die Firewall, um den Zugriff auf den Server mittels Web Console nur von vertrauenswürdigen Geräten zu erlauben.
- Konfigurieren Sie das TLS-Protokoll in Version 1.2 oder höher auf dem Server.
- Konfigurieren Sie eine Firewall, um den Zugriff auf das Gerät mit dem installierten DBMS des Servers einzuschränken.
- Konfigurieren Sie die SSL-Authentifizierung zwischen dem Server und dem DBMS (MySQL oder PostgreSQL).

Benutzerkonten und Autorisierung

- Konfigurieren Sie Zwei-Faktor-Authentifizierung (TOTP, RFC 6238) für den Serverzugriff.
- Installieren Sie die Authentifikator-Anwendung nicht auf demselben Gerät, von dem aus die Verbindung zum Server über die Web Console hergestellt wird.
- Verwenden Sie für den Zugriff auf den Server eine Multi-Faktor-Authentifizierung (MFA) anhand eines Tokens, einer Smartcard oder Ähnlichem.
- Erstellen Sie eine dedizierte Administrationsgruppe für das Gerät des Servers und erstellen Sie eine spezielle Sicherheitsrichtlinie dafür.
- Schränken Sie die Anzahl der Benutzer mit der Rolle "Hauptadministrator" ein.
- Konfigurieren Sie die Berechtigungen zum Zugriff auf Serverfunktionen basierend auf Rollen von Benutzern und Gruppen.
- Erlauben Sie die Remote-Installation von Anwendungen nur für ein separates Benutzerkonto.
- Überprüfen Sie regelmäßig auf dem Gerät des Servers alle Benutzer.

Verwaltung des Schutzes des Administrationsservers

- Installieren Sie auf dem Gerät des Servers eine Sicherheitsanwendung:
  - Für einen physischen Server: Kaspersky Endpoint Security
  - Für einen virtuellen Server: Kaspersky Security for Virtualization

- Erstellen Sie eine separate Richtlinie für den Schutz des Servers und wenden Sie diese an (separat von den Sicherheitsrichtlinien anderer verwalteter Geräte).
- Aktivieren Sie in der Sicherheitsanwendung alle verfügbaren Schutzmodule.

Erstellung von Richtlinien und Aufgaben für verwaltete Kaspersky-Anwendungen

- Erstellen und wenden Sie Richtlinien für die folgenden Anwendungen auf alle verwalteten Geräte oder auf die Gruppe mit neuen verwalteten Geräten an:
  - Administrationsagent
  - Kaspersky Endpoint Security für Windows/Linux/macOS
  - Kaspersky Endpoint Agent (oder andere Kaspersky-Anwendungen)
- Aktivieren Sie den Kennwortschutz gegen die Deaktivierung des Schutzes oder die Deinstallation von Kaspersky-Anwendungen.
- Sperren Sie die Richtlinieneinstellungen (schließen Sie das "Schloss"), um zu verhindern, dass diesen Einstellungen auf verwalteten Geräten Änderungen zugewiesen werden.
- Erstellen Sie eine geplante Aufgabe zur vollständigen Untersuchung aller Geräte.
- Aktivieren Sie die Verwendung von Kaspersky Security Network (KSN) und akzeptieren Sie die aktuellste KSN-Erklärung.
- Konfigurieren Sie die Gerätesuche und geben Sie eine Standard-Administrationsgruppe für neu erkannte Geräte an.
- Schränken Sie die Verwendung automatischer Regeln für das Verschieben von Geräten zwischen Administrationsgruppen ein.
- Schützen Sie Verteilungspunkte vor unbefugtem Zugriff.
- Vermeiden Sie die automatische Zuweisung von Verteilungspunkten in kleinen oder kritischen Netzwerken.

Wartung des Administrationsservers

- Löschen oder deaktivieren Sie nicht die folgenden Aufgaben:
  - Backup
  - Wartung des Administrationsservers
- Installieren Sie regelmäßig Updates für das Betriebssystem und die Software von Drittanbietern.

Übertragung von Ereignissen an Systeme von Drittanbietern

- Konfigurieren Sie die Überwachung und Berichterstattung von Sicherheitsereignissen.
- Konfigurieren Sie den Export von Ereignissen in ein SIEM-System.

- Konfigurieren Sie Serverbenachrichtigungen für:
  - Audit-Ereignisse
  - Kritische Ereignisse
  - Fehlerereignisse und Warnungen

Sicherheitsempfehlungen für Drittanbieter-Informationssysteme

- Wenden Sie die Sicherheitsempfehlungen der CIS-Benchmarks auf die verwendeten Betriebssysteme, DBMS und Hypervisoren an.
- Befolgen Sie für Astra Linux die Sicherheitsempfehlungen der entsprechenden Version des Red Books.
- Befolgen Sie für RED OS die Empfehlungen aus der offiziellen RED OS-Dokumentation.

Bereitstellung des Administrationsservers

Architektur des Administrationsservers

Im Allgemeinen hängt die Wahl einer zentralisierten Verwaltungsarchitektur von Punkten wie dem Standort der geschützten Geräte, dem Zugriff von benachbarten Netzwerken und den Bereitstellungsschemata für Datenbankaktualisierungen ab.

In der Anfangsphase der Architekturentwurfs empfehlen wir, sich mit den Komponenten von Kaspersky Security Center Linux und ihren Wechselwirkungen untereinander, sowie mit den Schemata für Datenverkehr und Portnutzung vertraut zu machen.

Basierend auf diesen Informationen können Sie eine Architektur entwerfen, die auf Folgendes eingeht:

- Standort des Administrationsservers und Netzwerkverbindungen
- Organisation der Arbeitsbereiche des Administrators und Verbindungsmethoden zum Administrationsserver
- Methoden zur Bereitstellung des Administrationsagenten und der Schutzprogramme
- Verwendung von Verteilungspunkten
- Verwendung von virtuellen Administrationsservern
- Verwendung einer Administrationsserver-Hierarchie
- Update-Schema für Antiviren-Datenbanken
- Weitere Datenflüsse

Auswahl eines Geräts zur Installation des Administrationsservers

Wir empfehlen, dass Sie den Administrationsserver auf einem dedizierten Server in der Infrastruktur Ihrer Organisation installieren. Wenn auf dem Server keine weiteren Drittanbieter-Programme installiert sind, können Sie die Sicherheitseinstellungen gemäß den Anforderungen von Kaspersky Security Center Linux konfigurieren, ohne von den Anforderungen der Drittanbieter-Programme abhängig zu sein.

Sie können den Administrationsserver auf einem physischen Server oder auf einem virtuellen Server bereitstellen. Stellen Sie sicher, dass das ausgewählte Gerät die Hardware- und Softwareanforderungen erfüllt.

Einschränkung bei der Bereitstellung des Administrationsservers auf einem Domänencontroller, Terminalserver oder Benutzergerät

Wir raten dringend davon ab, den Administrationsserver auf einem Domänencontroller, Terminalserver oder Benutzergerät zu installieren.

Wir empfehlen, dass Sie für die Schlüsselknoten des Netzwerks eine funktionale Trennung vorzusehen. Mit diesem Ansatz können Sie die Funktionsfähigkeit verschiedener Systeme aufrechterhalten, wenn ein Knoten ausfällt oder kompromittiert wird. Gleichzeitig können Sie für jeden Knoten unterschiedliche Sicherheitsrichtlinien erstellen.

Konten für die Installation und Ausführung des Administrationsservers

Während der Bereitstellung des Administrationsservers ist es erforderlich, zwei nicht privilegierte Benutzerkonten zu erstellen. Die im Administrationsserver enthaltenen Dienste werden unter diesen nicht privilegierten Benutzerkonten ausgeführt. Befolgen Sie das Prinzip der geringsten Rechte, wenn Sie den Konten Rechte und Berechtigungen erteilen. Vermeiden Sie es, unnötige Benutzerkonten in die Gruppe "kladmins" aufzunehmen.

Zudem müssen Sie ein internes DBMS-Konto erstellen. Der Administrationsserver verwendet dieses interne DBMS-Benutzerkonto, um auf das ausgewählte DBMS zuzugreifen.

Art und Umfang der erforderlichen Benutzerkonten und deren Rechte hängen vom ausgewählten DBMS-Typ und der Methode zur Erstellung der Administrationsserver-Datenbank ab.

Verbindungssicherheit

Verwendung von TLS

Wir empfehlen, unsichere Verbindungen zum Administrationsserver zu verbieten. Beispielsweise können Sie in den Einstellungen des Administrationsservers Verbindungen verbieten, die HTTP verwenden.

Beachten Sie, dass standardmäßig einige HTTP-Ports des Administrationsservers geschlossen sind. Der verbleibende Port wird für den Webserver des Administrationsservers (8060) verwendet. Dieser Port kann durch die Firewall-Einstellungen des Administrationsservers eingeschränkt werden.

Restriktive TLS-Einstellungen

Wir empfehlen, das TLS-Protokoll ab Version 1.2 zu verwenden und unsichere Verschlüsselungsalgorithmen einzuschränken oder zu verbieten.

Sie können die vom Administrationsserver verwendeten Verschlüsselungsprotokolle konfigurieren (TLS). Beachten Sie, dass zum Veröffentlichungszeitpunkt einer Administrationsserver-Version die Einstellungen des Verschlüsselungsprotokolls standardmäßig so konfiguriert sind, dass sie eine sichere Datenübertragung gewährleisten.

Einschränkung des Zugriffs auf die Administrationsserver-Datenbank

Wir empfehlen eine Einschränkung des Zugriffs auf die Administrationsserver-Datenbank. Beispielsweise können Sie den Zugriff lediglich vom Gerät des Administrationsservers aus zulassen. Dadurch wird die Wahrscheinlichkeit verringert, dass die Administrationsserver-Datenbank aufgrund bekannter Schwachstellen kompromittiert wird.

Sie können die Parameter gemäß dem Handbuch der verwendeten Datenbank konfigurieren sowie geschlossene Ports auf Firewalls bereitstellen.

Sichere Interaktion mit einem externen DBMS

Wenn das DBMS während der Installation des Administrationsservers auf einem separaten Gerät installiert wird (externes DBMS), wird es empfohlen, die Parameter für die sichere Interaktion und Authentifizierung mit diesem DBMS anzupassen. Weitere Informationen über die Konfiguration der SSL-Authentifizierung finden Sie im Szenario: Authentifizierung am PostgreSQL-Server und im Szenario: Authentifizierung am MySQL-Server.

Eine Allow-Liste von IP-Adressen für die Verbindung mit dem Administrationsserver konfigurieren

Standardmäßig können sich Benutzer von Kaspersky Security Center Linux auf jedem Gerät, auf dem die Kaspersky Security Center Web Console oder OpenAPI-Anwendungen installiert sind, bei Kaspersky Security Center Linux anmelden. Sie können den Administrationsserver auch so konfigurieren, dass Benutzer nur von Geräten mit zugelassenen IP-Adressen eine Verbindung zu ihm herstellen dürfen. Wenn beispielsweise eine angreifende Person versucht, sich bei Kaspersky Security Center Linux mittels eines Servers von Kaspersky Security Center Web Console anzumelden, der auf einem Gerät installiert ist, das nicht auf der Allow-Liste steht, kann sich diese Person nicht an Kaspersky Security Center Linux anmelden.

Allow-Liste mit IP-Adressen für die Verbindung mit Kaspersky Security Center Web Console konfigurieren

Standardmäßig können sich Benutzer von Kaspersky Security Center Linux von jedem Gerät aus mit der Kaspersky Security Center Web Console verbinden. Auf einem Gerät mit Kaspersky Security Center Web Console müssen Sie eine Firewall konfigurieren (via Betriebssystem oder Drittanbieter-Anwendung), damit sich Benutzer nur mit erlaubten IP-Adressen mit der Kaspersky Security Center Web Console verbinden können.

Sicherheit der Verbindung mit dem Domänencontroller während der Abfrage

Um den Domänencontroller abzufragen, versucht der Administrationsserver oder ein Linux-Verteilungspunkt, sich mittels LDAPS mit der Domäne zu verbinden. Standardmäßig ist bei der Verbindung keine Überprüfung des Zertifikats notwendig. Um die Überprüfung des Zertifikats zu erzwingen, setzen Sie das Flag `KLNAG_LDAP_TLS_REQCERT` auf "1". Sie können außerdem einen benutzerdefinierten Pfad zur Zertifizierungsstelle (CA) angeben, um über das Flag `KLNAG_LDAP_SSL_CACERT` auf die Zertifikatkette zuzugreifen.

Konten und Authentifizierung

Bevor Sie die folgenden Schritte ausführen, erstellen Sie eine Backup-Kopie des Kaspersky Security Center Linux Administrationsservers mithilfe der Aufgabe Backup der Daten des Administrationsservers anlegen oder des Tools "klbackup" und speichern Sie diese an einem sicheren Ort.

Verwendung der Zwei-Faktor-Authentifizierung mit dem Administrationsserver

Kaspersky Security Center Linux verwendet die Zwei-Faktor-Authentifizierung bei der Anmeldung an der Kaspersky Security Center Web Console, basierend auf dem Standard RFC 6238 (TOTP: Time-Based One-Time Password-Algorithmus).

Jedes Mal, wenn Sie sich bei der Kaspersky Security Center Web Console anmelden, geben Sie Ihren Benutzernamen, Ihr Passwort und einen zusätzlichen Einmal-Sicherheitscode ein. Um einen Einmal-Sicherheitscode zu erhalten, müssen Sie eine Authenticator-App auf Ihrem Computer oder Mobilgerät installieren.

Für den RFC 6238-Standard existieren sowohl Software- als auch Hardware-Authenticators (Token). Zu den Software-Authenticators gehören beispielsweise Google Authenticator, Microsoft Authenticator und FreeOTP.

Wir raten dringend davon ab, die Authenticator-App auf demselben Gerät zu installieren, von dem aus die Verbindung zum Administrationsserver hergestellt wird. Sie können eine Authenticator-App auf Ihrem Mobilgerät installieren.

Verwendung der Zwei-Faktor-Authentifizierung für ein Betriebssystem

Um einen umfassenden Schutz durch die Zwei-Faktor-Authentifizierung zu gewährleisten, muss nicht nur der Administrationsserver, sondern auch das Gerät, auf dem er installiert ist, gesichert werden.

Wenn Sie eine Verbindung zu dem Gerät herstellen, auf dem der Administrationsserver installiert ist (über SSH, RDP oder andere Protokolle), empfehlen wir die Verwendung einer Multi-Faktor-Authentifizierung (MFA) mit einem Token, einer Smartcard oder einer anderen Authentifizierungsmethode.

Speichern des Administratorkennworts einschränken

Wenn Sie Kaspersky Security Center Web Console verwenden, raten wir davon ab, das Administratorkennwort in einem auf dem Benutzergerät installierten Browser zu speichern.

Authentifizierung eines internen Benutzerkontos

Standardmäßig muss das Kennwort eines internen Benutzerkontos des Administrationsservers die folgenden Regeln einhalten:

- Das Kennwort muss zwischen 8 und 256 Zeichen lang sein
- Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:

- Großbuchstaben (A–Z)
- Kleinbuchstaben (a–z)
- Ziffern (0–9)
- Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

Standardmäßig liegt die maximale Anzahl zulässiger Versuche zur Eingabe eines Kennworts bei 10. Sie können die Anzahl der zulässigen Eingabeversuche für das Kennwort ändern.

Die Benutzer von Kaspersky Security Center Linux haben nur eine begrenzte Anzahl von Eingabeversuchen mit ungültigen Kennwörtern. Wenn das Limit erreicht ist, wird das Benutzerkonto für eine Stunde gesperrt.

Optionen zur Kennwortänderung eines internen Benutzerkontos konfigurieren

Es wird empfohlen, die folgenden Optionen für die Kennwortänderung eines internen Benutzerkontos zu konfigurieren:

- Zeitraum der Kennwortrotation
- Zeitspanne der vorherigen Warnung über eine erforderliche Kennwortänderung
- Wert der Option **Benutzer muss bei Erstanmeldung sein Kennwort ändern**

Schutz von Benutzerkonten vor unbefugten Änderungen

Es wird empfohlen, eine zusätzliche Option zu aktivieren, um interne Benutzerkonten des Administrationsservers unbefugter Änderung zu schützen. Dieser Schutz muss für jeden internen Benutzer separat konfiguriert werden.

Dedizierte Administrationsgruppe für den Administrationsserver

Wir empfehlen die Erstellung einer dedizierten Administrationsgruppe für den Administrationsserver. Gewähren Sie dieser Gruppe gesonderte Zugriffsrechte und erstellen Sie eine gesonderte Sicherheitsrichtlinie für sie.

Um die Sicherheitsstufe des Administrationsservers nicht absichtlich herabzusetzen, empfehlen wir, die Liste der Konten einzuschränken, welche die dedizierte Administrationsgruppe verwalten dürfen.

Zuweisung der Rolle "Hauptadministrator" beschränken

Dem mit dem Tool "kladduser" erstellten Benutzer wird in der Zugriffskontrollliste (ACL) des Administrationsservers oder des virtuellen Administrationsservers die Rolle "Hauptadministrator" zugewiesen. Es wird empfohlen, die Zuweisung der Rolle des Hauptadministrators an eine größere Anzahl von Benutzern zu vermeiden.

Zugriffsrechte auf Programmfunktionen konfigurieren

Wir empfehlen, für jeden Benutzer oder jede Benutzergruppe eine flexible Konfiguration der Zugriffsrechte auf die Funktionen von Kaspersky Security Center Linux.

Rollenbasierte Zugriffskontrolle erlaubt das Erstellen typischer Benutzerrollen mit einer vordefinierten Auswahl von Berechtigungen und das Zuweisen dieser Rollen an die Benutzer entsprechend ihrer dienstlichen Verpflichtungen.

Die Hauptvorteile des Modells der rollenbasierten Zugriffskontrolle:

- Einfache Verwaltung
- Rollenhierarchie
- Prinzip der niedrigsten Priorität (POLP)
- Trennung von Aufgaben

Sie können bestimmten Mitarbeitern basierend auf deren Positionen vordefinierte Rollen zuweisen oder neue Rollen erstellen.

Achten Sie bei der Rollenkonfiguration auf die Berechtigungen, die mit der Änderung des Schutzstatus des Geräts mit dem Administrationsserver und der Remote-Installation von Drittanbieter-Programmen verbunden sind:

- Administrationsgruppen verwalten.
- Vorgänge mit dem Administrationsserver.
- Remote-Installation.
- Ändern der Parameter zum Speichern von Ereignissen und Senden von Benachrichtigungen.

  Mit diesem Recht können Sie Benachrichtigungen einrichten, die bei Eintritt eines Ereignisses ein Skript oder ein ausführbares Modul auf dem Gerät des Administrationsservers ausführen.

Separate Benutzerkonten für die Remote-Installation von Programmen

Neben der grundsätzlichen Unterscheidung der Zugriffsrechte empfehlen wir, die Remote-Installation von Programmen für alle Konten einzuschränken (außer für den Hauptadministrator oder ein anderes spezialisiertes Konto).

Für die Remote-Installation von Anwendungen empfehlen die Verwendung eines separaten Benutzerkontos. Sie können dem separaten Benutzerkonto Berechtigungen oder eine Rolle zuweisen.

Regelmäßiges Audit aller Benutzer und Benutzervorgänge

Wir empfehlen, auf dem Gerät des Administrationsservers eine regelmäßige Überprüfung aller Benutzer durchzuführen. Auf diese Weise können Sie auf bestimmte Arten von Sicherheitsbedrohungen reagieren, die mit einer möglichen Kompromittierung des Geräts verbunden sind.

Außerdem können Sie verschiedene Benutzervorgänge verfolgen, wie etwa: hergestellte und getrennte Verbindungen zum Administrationsserver, fehlerhafte Verbindungen zum Administrationsserver und Objektänderungen (für Objekte, welche die Revisionsverwaltung unterstützen).

Verwaltung des Schutzes des Administrationsservers

Auswahl eines Schutzprogramms für den Administrationsserver

Wählen Sie je nach Einsatzart des Administrationsservers und der allgemeinen Schutzstrategie die Anwendung aus, die das Gerät des Administrationsservers schützen soll.

Wenn Sie den Administrationsserver auf einem dezidierten Gerät bereitstellen, empfehlen wir, Kaspersky Endpoint Security als Anwendung für den Schutz des Geräts mit dem Administrationsserver auszuwählen. Dies ermöglicht die Verwendung aller verfügbaren Technologien zum Schutz des Geräts des Administrationsservers, einschließlich den Modulen zur Verhaltensanalyse.

Wenn der Administrationsserver auf einem Gerät installiert wird, das in der Infrastruktur vorhanden ist und zuvor für andere Aufgaben verwendet wurde, empfehlen wir, die folgende Schutzanwendungen in Betracht zu ziehen:

- Kaspersky Industrial CyberSecurity for Nodes. Wir empfehlen, diese Anwendung auf Geräten zu installieren, die in ein industrielles Netzwerk eingebunden sind. Kaspersky Industrial CyberSecurity for Nodes ist eine Anwendung, die über Kompatibilitätszertifikate mit verschiedenen Herstellern von Industriesoftware verfügt.

- Empfohlene Sicherheitsprodukte. Wenn der Administrationsserver auf einem Gerät mit anderer Software installiert ist, empfehlen wir, die Empfehlungen dieses Softwareanbieters zur Kompatibilität von Sicherheitsprodukten zu berücksichtigen (möglicherweise gibt es bereits Empfehlungen zur Auswahl einer Sicherheitslösung, und Sie müssen möglicherweise die vertrauenswürdige Zone konfigurieren).

Erstellen einer separaten Sicherheitsrichtlinie für die Schutzanwendung

Wir empfehlen, dass Sie eine separate Sicherheitsrichtlinie für die Anwendung erstellen, die das Gerät mit dem Administrationsserver schützt. Diese Richtlinie muss sich von der Sicherheitsrichtlinie für Client-Geräte unterscheiden. Dadurch können die am besten geeigneten Sicherheitseinstellungen für den Administrationsserver festgelegt werden, ohne die Schutzstufe anderer Geräte zu beeinträchtigen.

Wir empfehlen, die Geräte in Gruppen zu unterteilen und anschließend das Gerät des Administrationsservers in einer separaten Gruppe zu platzieren, für die Sie eine spezielle Sicherheitsrichtlinie erstellen können.

Schutzmodule

Wenn es für die Drittanbieter-Programme, die auf dem Gerät mit dem Administrationsserver installiert sind, keine besonderen Empfehlungen vom Hersteller der gibt, empfehlen wir, alle verfügbaren Schutzmodule zu aktivieren und zu konfigurieren. Dem sollte ausreichend Zeit zur Überprüfung der Ausführung dieser Schutzmodule vorausgehen.

Konfiguration der Firewall des Administrationsserver-Geräts

Auf dem Gerät mit dem Administrationsserver empfehlen wir die Firewall so zu konfigurieren, dass die Anzahl derjenigen Geräte, von denen Administratoren über die Kaspersky Security Center Web Console eine Verbindung zum Administrationsserver herstellen können, eingeschränkt wird.

Standardmäßig verwendet der Administrationsserver den Port 13299, um Verbindungen von Kaspersky Security Center Web Console zu empfangen. Wir empfehlen, die Anzahl der Geräte zu beschränken, von denen der Administrationsserver über diesen Port verwaltet werden kann.

Verwaltung des Schutzes der Client-Geräte

Einschränken des Hinzufügens von Lizenzschlüsseln zu Installationspaketen

Installationspakete werden im freigegebenen Ordner des Administrationsservers im Unterordner "Pakete" gespeichert. Wenn Sie einem Installationspaket einen Lizenzschlüssel hinzufügen, können alle Benutzer mit Leserechten für diesen Ordner auf den Lizenzschlüssel zugreifen (direkt oder über den in den Administrationsserver integrierten Webserver).

Um eine Gefährdung des Lizenzschlüssels zu vermeiden, raten wir davon ab, Lizenzschlüssel zu den Installationspaketen hinzuzufügen.

Wir empfehlen für die Bereitstellung die Verwendung der automatischen Verteilung von Lizenzschlüsseln an verwaltete Geräte mithilfe der Aufgabe "Hinzufügen eines Lizenzschlüssels für ein verwaltetes Programm" und manuelles Hinzufügen eines Aktivierungscodes oder einer Schlüsseldatei zu den Geräten.

Automatische Regeln für das Verschieben von Geräten zwischen Administrationsgruppen

Wir empfehlen, die Verwendung automatischer Regeln für das Verschieben von Geräten zwischen Administrationsgruppen einzuschränken.

Wenn Sie automatische Regeln zum Verschieben von Geräten verwenden, kann dies zur Verbreitung von Richtlinien führen, die dem verschobenen Gerät mehr Berechtigungen gewähren, als das Gerät vor dem Verschieben besaß.

Darüber hinaus kann das Verschieben eines Client-Geräts in eine andere Administrationsgruppe zur Verbreitung von Richtlinieneinstellungen führen. Die Verteilung dieser Richtlinien an Gastgeräte und nicht vertrauenswürdige Geräte kann unerwünscht sein.

Diese Empfehlung gilt nicht für die einmalige erstmalige Zuordnung von Geräten zu Administrationsgruppen.

Sicherheitsanforderungen an Verteilungspunkte und Verbindungs-Gateways

Geräte mit installiertem Administrationsagenten können als Verteilungspunkt fungieren und die folgenden Funktionen ausführen:

- Vom Administrationsserver empfangene Updates und Installationspakete an die Client-Geräte innerhalb der Gruppe verteilen.
- Durchführen von Remote-Installationen von Drittanbieter-Programmen und Kaspersky-Anwendungen auf den Client-Geräten.
- Abfragen des Netzwerks, um neue Geräte und aktualisierte Informationen über die bereits bekannten Geräte zu finden. Der Verteilungspunkt kann dieselben Methoden zur Geräteerkennung verwenden wie der Administrationsserver.

Das Platzieren von Verteilungspunkten im Netzwerk der Organisation kann für Folgendes verwendet werden:

- Entlastung des Administrationsservers
- Optimierung des Datenverkehrs
- Gewähren von Zugriff für den Administrationsserver auf Geräte, die sich an schwer erreichbaren Standorten des Unternehmensnetzwerks befinden

Unter Berücksichtigung der verfügbaren Funktionen empfehlen wir, alle Geräte, die als Verteilungspunkte fungieren, vor jeglicher Art von unbefugtem Zugriff (einschließlich physischem) zu schützen.

Einschränken der automatischen Zuweisung von Verteilungspunkten

Um die Administration zu vereinfachen und die Funktionsfähigkeit des Netzwerks zu erhalten, empfehlen wir die automatische Zuweisung von Verteilungspunkten. Für industrielle Netzwerke und kleine Netzwerke empfehlen wir jedoch, die automatische Zuweisung von Verteilungspunkten zu vermeiden. Das liegt darin begründet, da beispielsweise die privaten Informationen der Konten, die zum Anstoßen von Remote-Installationsaufgaben verwendet werden, mithilfe von Betriebssystem-Ressourcen an Verteilungspunkte übertragen werden können.

Für industrielle Netzwerke und kleine Netzwerke ist es möglich Geräten manuell die Rolle als Verteilungspunkt zuweisen.

Sie können auch den Bericht über die Aktivität der Verteilungspunkte anzeigen.

Sicherheitsanforderungen an die Geräte der Benutzer von Kaspersky Security Center Linux

Für die Geräte der Benutzer von Kaspersky Security Center Linux müssen besondere Sicherheitsanforderungen gelten. Es wird empfohlen, diese Geräte vor jeglicher Art von unbefugtem Zugriff (auch physisch) zu schützen.

Die Geräte der Benutzer von Kaspersky Security Center Linux umfassen:

- Geräte, von denen sich Benutzer von Kaspersky Security Center Linux über einen Browser mit der Kaspersky Security Center Web Console verbinden.
- Geräte, von den sich Anwendungen, die mittels OpenAPI mit dem Administrationsserver kommunizieren, mit Kaspersky Security Center Linux verbinden.

Sicherheitsanforderungen an Geräte mit installierter Kaspersky Security Center Web Console

Geräte mit installierter Kaspersky Security Center Web Console werden zur Verwaltung von Kaspersky Security Center Linux verwendet. Es gelten daher besondere Sicherheitsanforderungen für diese Geräte. Es wird empfohlen, diese Geräte vor jeglicher Art von unbefugtem Zugriff (auch physisch) zu schützen.

Konfigurieren des Schutzes für verwaltete Programme

Verwaltete Richtlinien für Programme

Wir empfehlen das Erstellen einer Richtlinie für jede Art von verwendeten Anwendungen und Komponenten von Kaspersky Security Center Linux (Administrationsagent, Kaspersky Endpoint Security für Windows, Kaspersky Endpoint Security für Linux, Kaspersky Endpoint Agent und weitere). Diese Richtlinie muss auf alle verwalteten Geräte (Stamm-Administrationsgruppe "Verwaltete Geräte") oder auf eine separate Gruppe, in die neue verwaltete Geräte gemäß den konfigurierten Verschiebungsregeln automatisch verschoben werden, angewendet werden.

Festlegen eines Kennworts zum Deaktivieren des Schutzes und Deinstallieren des Programms

Es wird dringend empfohlen, den Kennwortschutz zu aktivieren, um zu verhindern, dass Angreifer die Kaspersky-Sicherheitsanwendungen deaktivieren oder deinstallieren. Auf Plattformen, auf denen der Kennwortschutz unterstützt wird, können Sie ein Kennwort beispielsweise für Kaspersky Endpoint Security, den Administrationsagenten und weitere Kaspersky-Programme festlegen. Nachdem Sie den Kennwortschutz aktiviert haben, empfehlen wir, die entsprechenden Einstellungen zu sperren, indem Sie das "Schloss" schließen.

Angeben des Kennworts für die manuelle Verbindung eines Client-Geräts mit dem Administrationsserver (Tool "klmover")

Mit dem Tool "klmover" können Sie ein Client-Gerät manuell mit dem Administrationsserver verbinden. Das Tool "klmover" befindet sich im Installationsordner des Administrationsagenten.

Um zu verhindern, dass Angreifer Geräte aus dem Kontrollbereich Ihres Administrationsservers heraus verschieben können, wird es dringend empfohlen, für die Ausführung des Tools "klmover" den Kennwortschutz zu aktivieren. Um den Kennwortschutz zu aktivieren, wählen Sie in den Richtlinieneinstellungen des Administrationsagenten die Option **Deinstallationskennwort verwenden**.

Das Tool "klmover" erfordert lokale Administratorrechte.

Wenn Sie für einen kennwortgeschützten Administrationsagenten auf einem Gerät, das nicht mehr von Kaspersky Security Center Linux verwaltet wird, das Kennwort verlieren oder vergessen, können Sie diesen Administrationsagenten weder mit den Tools "klmover" und "Cleaner" (cleaner.exe) noch über die Eingabeaufforderung entfernen. In diesem Fall müssen Sie auf dem Gerät mit installiertem kennwortgeschützten Administrationsagenten das Betriebssystem neu installieren.

Das Aktivieren der Option **Deinstallationskennwort verwenden** aktiviert auf Windows-Geräten ebenfalls den Kennwortschutz für das Cleaner-Tool (cleaner.exe).

Verwenden von Kaspersky Security Network

Wir empfehlen, in allen Richtlinien der verwalteten Programme und in den Eigenschaften des Administrationsservers die Verwendung von Kaspersky Security Network (KSN) zu aktivieren und die KSN-Erklärung zu akzeptieren. Wenn Sie den Administrationsserver aktualisieren, können Sie die aktualisierte KSN-Erklärung akzeptieren. In einigen Fällen können Sie KSN deaktivieren, z. B. wenn die Nutzung von Cloud-Diensten gesetzlich oder durch andere Vorschriften verboten ist.

Regelmäßiges Untersuchen verwalteter Geräte

Wir empfehlen, für alle Gerätegruppen eine Aufgabe zu erstellen, die regelmäßig eine vollständige Untersuchung der Geräte durchführt.

Suchen von neuen Geräten

Wir empfehlen die ordnungsgemäße Konfiguration der Einstellung der Suche nach Geräten: Richten Sie die Integration mit den Domänencontrollern ein und geben Sie Bereiche der IP-Adressen für die Suche nach neuen Geräten an.

Aus Sicherheitsgründen können Sie die standardmäßige Administrationsgruppe verwenden, die alle neuen Geräte sowie die Standardrichtlinien enthält, die diese Gruppe betreffen.

Wartung des Administrationsservers

Anlegen eines Daten-Backups für den Administrationsservers

Ein Daten-Backup ermöglicht die Wiederherstellung der Daten des Administrationsservers ohne Datenverlust.

Standardmäßig wird nach der Installation des Administrationsservers automatisch eine Aufgabe zum Anlegen eines Daten-Backups erstellt und regelmäßig ausgeführt, wobei Sicherungen im entsprechenden Verzeichnis gespeichert werden.
Der Einstellungen der Aufgabe zum Anlegen eines Daten-Backups können wie folgt geändert werden:

- Die Frequenz des Datensicherung kann erhöht werden
- Es kann ein spezielles Verzeichnis zum Speichern von Kopien angegeben werden
- Kennwörter für Sicherungskopien können geändert werden

Wenn Sie Sicherungskopien in einem speziellen Verzeichnis ablegen, das sich vom Standardverzeichnis unterscheidet, empfehlen wir, die Zugriffskontrollliste (ACL) für dieses Verzeichnis einzuschränken. Die Konten für den Administrationsservers und für die Administrationsserver-Datenbank müssen Schreibzugriff auf dieses Verzeichnis haben.

Wartung des Administrationsservers

Durch die Wartung des Administrationsservers können Sie die Datenbankgröße reduzieren sowie die Leistungsfähigkeit und die Zuverlässigkeit des Programms verbessern. Es wird empfohlen, den Administrationsserver mindestens einmal pro Woche zu warten.

Die Wartung des Administrationsservers erfolgt mithilfe der entsprechenden Aufgaben. Bei der Wartung des Administrationsservers führt das Programm die folgenden Aktionen aus:

- Datenbanken neu indizieren
- Datenbankstatistik aktualisieren
- Datenbank komprimieren (falls erforderlich)

Updates für das Betriebssystem und für Drittanbieter-Programme installieren

Wir empfehlen dringend, auf dem Gerät mit dem Administrationsserver regelmäßig Updates für das Betriebssystem und für Drittanbieter-Programme zu installieren.

Client-Geräte benötigen keine ständige Verbindung zum Administrationsserver, daher ist es sicher, das Gerät mit dem Administrationsserver nach einer Update-Installation neu zu starten. Alle auf den Client-Geräten während einer Downtime des Administrationsservers registrierten Ereignisse werden nach Wiederherstellung der Verbindung an den Administrationsserver gesendet.

Ereignisübertragung an Systeme von Dritten

Überwachung und Berichterstattung

Um rechtzeitig auf Sicherheitsprobleme reagieren zu können, empfehlen wir, die Funktion Überwachung und Berichterstattung zu konfigurieren.

Ereignisse in SIEM-Systeme exportieren

Um Sicherheitsprobleme schnell zu erkennen und das Entstehen größerer Schäden zu vermeiden, empfehlen wir die Verwendung des Ereignisexports in ein SIEM-System.

E-Mail-Benachrichtigungen über Audit-Ereignisse

Kaspersky Security Center Linux ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Kaspersky-Anwendungen aufgetreten sind. Um rechtzeitig auf Notfälle reagieren zu können, empfehlen wir, den Administrationsserver so zu konfigurieren, dass er Benachrichtigungen über die von ihm veröffentlichten Audit-Ereignisse, kritischen Ereignisse, Fehlermeldungen und Warnungen sendet.

Da es sich bei diesen Ereignissen um interne System-Ereignisse handelt, ist mit einer geringen Anzahl von ihnen zu rechnen, was einem Versenden per Mail entgegenkommt.

Sicherheitsempfehlungen für Drittanbieter-Informationssysteme

Sicherheitsempfehlungen für CIS-Benchmarks

Wenn Sie die vom Administrationsserver und vom Administrationsagenten unterstützten Versionen der Betriebssysteme, Virtualisierungsplattformen oder Datenbankserver einsetzen und diese Informationssysteme genauer anpassen möchten, empfehlen wir die bewährten Verfahren für Informationssicherheit des Center for Internet Security (CIS) (sofern vorhanden).

Das Center for Internet Security (CIS) ist eine gemeinnützige Organisation, die sich der Verbesserung der Sicherheit im Bereich der Informationstechnologie verschrieben hat. Insbesondere werden vom CIS Sicherheitsstandards wie die CIS Controls und CIS Benchmarks entwickelt und zur Verfügung gestellt. Diese Standards sind eine Reihe von Empfehlungen und Praktiken zur Gewährleistung der Sicherheit von Informationssystemen.

Das CIS-Portal enthält Empfehlungen für die Versionen der folgenden Informationssysteme, die vom Administrationsserver und vom Administrationsagenten unterstützt werden:

- Betriebssysteme aus folgenden Familien:
  - Windows für Desktops
  - Windows für Server
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- VMware-Virtualisierungsplattformen
- Datenbankserver:
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Sicherheitsempfehlungen für das Betriebssystem Astra Linux

Wenn Sie das Betriebssystem Astra Linux verwenden, sollten Sie die Sicherheitsempfehlungen befolgen, die im Red Book der entsprechenden Version von Astra Linux (auf Russisch) beschrieben sind.

Sicherheitsempfehlungen für das Betriebssystem RED OS

Wenn Sie das Betriebssystem RED OS verwenden, sollten Sie die in der offiziellen Dokumentation zu RED OS beschriebenen Sicherheitsempfehlungen des Administratorhandbuchs befolgen.

Empfehlungen für die Verwendung von Kaspersky-Sicherheitsanwendungen

Verwendung des KLAdmin-Kennworts in Kaspersky Endpoint Security für Windows

Das KLAdmin-Konto ist ein Administratorkonto mit uneingeschränktem Zugriff auf Kaspersky Endpoint Security für Windows. Das Benutzerkonto "KLAdmin" ist dazu berechtigt, sämtliche kennwortgeschützten Vorgänge in Kaspersky Endpoint Security für Windows auszuführen, einschließlich der Deinstallation der Anwendung. Die Berechtigungen für das KLAdmin-Konto können nicht widerrufen werden. Sie können das Kennwort für das KLAdmin-Konto in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows festlegen. Der Administrator von Kaspersky Endpoint Security für Windows ist voll verantwortlich für die sichere Verwendung des Kennworts für das KLAdmin-Konto. Wenn Ihr Unternehmen eine eigene Kennwortrichtlinie besitzt, beachten Sie die Anweisungen dieser Richtlinie. Je länger und komplexer das Kennwort ist, desto zuverlässiger ist es.

Unsere Empfehlungen für den Schutz einer Organisation vor dem Diebstahl des KLAdmin-Kennworts lauten wie folgt:

- **Allgemeine Anforderungen**

  Verwenden Sie weder den gesamten Kontonamen noch einen Teil des Namens als Kennwort.

- **Minimale Länge des Kennworts**

  Das Kennwort muss mindestens 10 Zeichen lang sein.

- **Obligatorische Zeichenkategorien**

  Legen Sie ein komplexes Kennwort mit Zeichen aus unterschiedlichen Kategorien fest: Klein- und Großbuchstaben, Ziffern und Sonderzeichen.

- **Gültigkeitsdauer des Kennworts**

  Legen Sie für das Kennwort eine Gültigkeitsdauer von mindestens 90 Tagen fest. Ein neues Kennwort darf nicht mit einem der letzten 24 Kennwörter übereinstimmen.

Szenario: Authentifizierung am MySQL-Server

Es wird empfohlen, für die Authentifizierung am MySQL-Servers ein TLS-Zertifikat zu verwenden. Sie können ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (certificate authority - CA) oder ein selbstsigniertes Zertifikat verwenden.

Der Administrationsserver unterstützt für MySQL sowohl die unidirektionale als auch die bidirektionale SSL-Authentifizierung.

Aktivieren der unidirektionalen SSL-Authentifizierung

Gehen Sie folgendermaßen vor, um die unidirektionale SSL-Authentifizierung für MySQL zu konfigurieren:

1. **Generieren Sie ein selbstsigniertes TLS-Zertifikat für den MySQL-Server**

   Führen Sie den folgenden Befehl aus:

```
openssl genrsa 1024 > ca-key.pem

openssl req -new -x509 -nodes -days 365 -key ca-key.pem -config myssl.cnf > ca-cert.pem

openssl req -newkey rsa:1024 -days 365 -nodes -keyout server-key.pem -config myssl.cnf
> server-req.pem

openssl x09 -req -in server-req.pem -days 365 -CA ca-cert.pem -CAkey ca-key.pem -
set_serial 01 > server-cert.pem
```

2. **Erstellen Sie eine Server-Flag-Datei**

   Verwenden Sie das Tool "klscflag", um das Server-Flag KLSRV_MYSQL_OPT_SSL_CA zu erstellen, und geben Sie den Pfad des Zertifikats als dessen Wert an. Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <Pfad zu ca-cert.pem> -t d
   ```

3. **Konfigurieren Sie die Datenbank**

   Geben Sie die Zertifikate in der Datei "my.cnf" an. Öffnen Sie die Datei "my.cnf" in einem Texteditor und fügen Sie im Abschnitt "[mysqld]" die folgenden Zeilen hinzu:

   ```
   [mysqld]

   ssl-ca=".../mysqlcerts/ca-cert.pem"

   ssl-cert=".../mysqlcerts/server-cert.pem"

   ssl-key=".../mysqlcerts/server-key.pem"
   ```

Aktivieren der bidirektionalen SSL-Authentifizierung

Gehen Sie folgendermaßen vor, um die bidirektionale SSL-Authentifizierung für MySQL zu konfigurieren:

1. **Erstellen Sie Server-Flag-Dateien**

   Verwenden Sie das Tool "klscflag", um die Server-Flags zu erstellen, und geben Sie die Pfade der Zertifikate als deren Wert an.

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <Pfad zu ca-cert.pem> -t s

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <Pfad zu server-cert.pem> -t
   s

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <Pfad zu server-key.pem> -t
   s
   ```

   Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

2. **Geben Sie die Passphrase an (optional)**

   Wenn server-key.pem eine Passphrase erfordert, erstellen Sie das Flag KLSRV_MARIADB_OPT_TLS_PASPHRASE und geben Sie die Passphrase als dessen Wert an:

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <Passphrase> -t s
   ```

3. **Konfigurieren Sie die Datenbank**

   Geben Sie die Zertifikate in der Datei "my.cnf" an. Öffnen Sie die Datei "my.cnf" in einem Texteditor und fügen Sie im Abschnitt "[mysqld]" die folgenden Zeilen hinzu:

   ```
   [mysqld]
   ```

```
ssl-ca=".../mysqlcerts/ca-cert.pem"
ssl-cert=".../mysqlcerts/server-cert.pem"
ssl-key=".../mysqlcerts/server-key.pem"
```

Szenario: Authentifizierung am PostgreSQL-Server

Es wird empfohlen, für die Authentifizierung am PostgreSQL-Server ein TLS-Zertifikat zu verwenden. Sie können ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle (certificate authority - CA) oder ein selbstsigniertes Zertifikat verwenden.

Der Administrationsserver unterstützt für PostgreSQL sowohl die unidirektionale als auch die bidirektionale SSL-Authentifizierung.

Die Authentifizierung von PostgreSQL Server erfolgt schrittweise:

1. **Generieren eines Zertifikats für den PostgreSQL-Server**

   Führen Sie die folgenden Befehle aus:

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj "/CN=psql"
   chmod og-rwx psql.key
   ```

2. **Generieren eines Zertifikats für den Administrationsserver**

   Führen Sie die folgenden Befehle aus. Der CN-Wert sollte mit dem Namen des Benutzers übereinstimmen, der sich im Namen des Administrationsservers mit PostgreSQL verbindet. Der Benutzername ist standardmäßig auf "postgres" eingestellt.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
   chmod og-rwx postgres.key
   ```

3. **Konfigurieren der Authentifizierung des Client-Zertifikats**

   Ändern Sie die Datei "pg_hba.conf" wie folgt:

   ```
   hostssl mydb myuser 192.168.1.0/16 scram-sha-256
   ```

   Stellen Sie sicher, dass die Datei "pg_hba.conf" keinen Eintrag enthält, der mit `host` beginnt.

4. **Angeben des PostgreSQL-Zertifikats**

   Für die unidirektionale SSL-Authentifizierung

   Ändern Sie die Datei "postgresql.conf" wie folgt (geben Sie den korrekten Pfad zu den crt- und key-Dateien an):

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

   Für die bidirektionale SSL-Authentifizierung

   Ändern Sie die Datei "postgresql.conf" wie folgt (geben Sie die korrekten Pfade zu den crt- und key-Dateien an):

```
listen_addresses ='localhost, server-ip'
ssl = on
ssl_ca_file = '<postgres.crt>'
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

5. **Neustarten des PostgreSQL-Daemons**

   Führen Sie den folgenden Befehl aus:

   ```
   systemctl restart postgresql-14.service
   ```

6. **Angeben des Server-Flags für den Administrationsserver.**

   Für die unidirektionale SSL-Authentifizierung

   Verwenden Sie das Tool "klscflag", um das Server-Flag KLSRV_POSTGRES_OPT_SSL_CA zu erstellen, und geben Sie den Pfad des Zertifikats als dessen Wert an.

   Öffnen Sie die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

   Führen Sie den folgenden Befehl aus:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <Pfad zu psql.crt> -t s
   ```

   Für die bidirektionale SSL-Authentifizierung

   Verwenden Sie das Tool "klscflag", um die Server-Flags zu erstellen, und geben Sie die Pfade der Zertifikate als deren Wert an.

   Öffnen Sie die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

   Führen Sie die folgenden Befehle aus:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <Pfad zu psql.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <Pfad zu
   postgres.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <Pfad zu postgres.key>
   -t s
   ```

   Wenn `postgres.key` eine Passphrase erfordert, erstellen Sie das Flag KLSRV_POSTGRES_OPT_TLS_PASPHRASE und geben Sie die Passphrase als dessen Wert an:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <Passphrase> -t
   s
   ```

7. **Neustarten des Dienstes des Administrationsservers**

Vorbereitung der Bereitstellung

In diesem Abschnitt wird beschrieben, wie Sie die Optionen zur Bereitstellung und Konfiguration von Kaspersky Security Center Linux und das zu verwendende DBMS entsprechend den Anforderungen Ihrer Organisation auswählen.

Um Kaspersky Security Center Linux im Netzwerk einer Organisation bereitzustellen, stehen mehrere Optionen zur Verfügung, die von den folgenden Kriterien abhängig sind:

- Gesamtzahl der Geräte
- Existenz von Unternehmens- oder geographisch isolierten Abteilungen (Büros, Filialen)
- Existenz von isolierten Netzwerken, die über enge Kanäle verbunden sind
- Notwendigkeit des Zugriffs auf den Administrationsserver über das Internet

Ein Administrationsserver unterstützt maximal 50.000 Geräte (mit PostgreSQL oder Postgres Pro als DBMS). Wenn die Gesamtzahl der Geräte im Unternehmensnetzwerk 50.000 überschreitet, müssen im Unternehmensnetzwerk mehrere Administrationsserver verteilt werden. Diese werden zur einfacheren zentralisierten Verwaltung in einer Hierarchie zusammengefasst.

Wenn es in der Zusammensetzung des Unternehmens große, geographisch voneinander entfernte Büros (Filialen) mit eigenen Administratoren gibt, es ist zweckmäßig, in diesen Büros Administrationsserver zu implementieren. Andernfalls müssen solche Büros wie isolierte Netzwerke betrachtet werden, die über Kanäle mit niedrigem Durchsatz verbunden sind (siehe Artikel "Typische Konfiguration: Mehrere größere Büros mit eigenen Administratoren").

Bei Vorhandensein von isolierten Netzwerken, die über enge Kanäle verbunden sind, müssen zwecks Optimierung des Datenverkehrs in solchen Netzwerken ein oder mehrere Administrationsagenten als Verteilungspunkte bestimmt werden (s. Tabelle zur Berechnung der Anzahl der Verteilungspunkte). In diesem Fall erhalten alle Geräte in einem isolierten Netzwerk die Updates von solchen "lokalen Update-Zentren". Die Verteilungspunkte können die Updates sowohl vom Administrationsserver (Standardszenario) als auch von den im Internet verfügbaren Servern von Kaspersky herunterladen (siehe Artikel "Typische Konfiguration: Mehrere kleine Remote-Büros").

Im Abschnitt Typische Konfigurationen von Kaspersky Security Center Linux erhalten Sie ausführliche Beschreibungen der typischen Konfigurationen von Kaspersky Security Center Linux. Bei der Planung der Bereitstellung muss je nach der Struktur des Unternehmens, die am geeignetste typische Konfiguration ausgewählt werden.

Bei der Planung der Bereitstellung muss die Notwendigkeit zur Angabe des speziellen Zertifikates X.509 für den Administrationsserver in Betracht gezogen werden. Die Angabe des Zertifikates X.509 für den Administrationsserver kann in folgenden Fällen (unvollständige Liste) zweckmäßig sein:

- Zur Untersuchung des SSL-Datenverkehres mittels SSL Termination Proxy oder zur Nutzung von Reverse Proxy
- Zur Integration der PKI-Infrastruktur (PKI) des Unternehmens
- Zur Angabe der gewünschten Werte für die Felder des Zertifikats
- Zur Gewährleistung der erwünschten Verschlüsselungsstärke des Zertifikats

Konfiguration von Kaspersky Security Center Linux auswählen

In diesem Abschnitt werden die folgenden typischen Konfigurationen für die Verteilung der Komponenten von Kaspersky Security Center Linux im Unternehmensnetzwerk beschrieben:

- Einzelbüro
- Mehrere große, geographisch verteilte Büros mit eigenen Administratoren
- Eine Menge kleine, geographisch verteilte Büros

Typische Konfiguration: Einzelbüro

Im Netzwerk des Unternehmens können ein oder mehrere Administrationsserver vorhanden sein. Die Anzahl der Administrationsserver kann sowohl ausgehend von der vorhandenen verfügbaren Hardware als auch in Abhängigkeit von der Gesamtmenge der verwalteten Geräte ausgewählt werden.

Ein Administrationsserver kann bis zu 50.000 Geräte unterstützen (mit PostgreSQL oder Postgres Pro als DBMS). Die Möglichkeit einer Erhöhung der Anzahl der verwalteten Geräte in nächster Zukunft muss berücksichtigt werden: es kann sich als wünschenswert erweisen, eine etwas kleinere Anzahl von Geräten mit einem Administrationsserver zu verbinden.

Die Administrationsserver können sich sowohl im internen Netzwerk als auch in der demilitarisierten Zone befinden, abhängig davon, ob ein Zugriff auf die Administrationsserver aus dem Internet erforderlich ist.

Wenn es mehrere Server gibt, ist es empfehlenswert, sie in einer Hierarchie zusammenzufassen. Durch Verwendung einer Hierarchie der Administrationsserver können Sie das Duplizieren von Richtlinien und Aufgaben vermeiden, und mit allen verwalteten Geräte arbeiten, als ob sie von einem einzigen Administrationsserver verwaltet würden (z. B. Geräte suchen, Geräteauswahlen erstellen und Berichte erstellen).

Typische Konfiguration: Mehrere größere Büros mit eigenen Administratoren

Für ein Unternehmen, das mehrere große Büros an unterschiedlichen Orten hat, sollten Sie die Option berücksichtigen, die Administrationsserver in jedem dieser Büros zu verteilen. In jedem Büro können ein oder mehrere Administrationsserver verteilt werden, abhängig von der Anzahl der Client-Geräte und der verfügbaren Hardware. In diesem Fall kann jedes Büros als Typische Einzelbüro-Konfiguration betrachtet werden. Um die Verwaltung zu vereinfachen, wird empfohlen, alle Administrationsserver in einer Hierarchie (ggf. mit mehreren Ebenen) zusammenzufassen.

Wenn einige Mitarbeiter mit ihren Geräten (Laptops) zwischen den Büros wechseln, können Sie Verbindungsprofile für den Administrationsagenten in der Richtlinie des Administrationsagenten erstellen.

Typische Konfiguration: Mehrere kleine Remote-Büros

Diese Standardkonfiguration ist vorgesehen für eine Unternehmenszentrale und zahlreiche kleine Remote-Büros, die über das Internet mit der Zentrale kommunizieren können. Die einzelnen Remote-Büros können sich hinter einer Netzwerkadressübersetzung (NAT) befinden. Das heißt, eine Verbindung zwischen zwei Remote-Büro ist nicht möglich, da die Büros voneinander isoliert sind.

In der Unternehmenszentrale muss ein Administrationsserver bereitgestellt werden, und ein oder mehrere Verteilungspunkte müssen allen übrigen Büros zugewiesen werden. Wenn eine Verbindung zwischen den Büros über das Internet hergestellt wird, kann es sinnvoll sein, für die Verteilungspunkte eine *Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte* zu erstellen, damit die Verteilungspunkte die Updates nicht vom Administrationsserver, sondern direkt von den Kaspersky-Servern oder lokalen oder Netzwerkordnern herunterladen.

Wenn im Remote-Büro ein Teil der Geräte keinen direkten Zugriff zum Administrationsserver hat (beispielsweise wenn der Zugriff auf den Administrationsserver durch das Internet erfolgt, aber nicht alle Geräte über Internetzugang verfügen), müssen die Verteilungspunkte in den Gateway-Modus (Verbindungs-Gateway) umgeschaltet werden. In diesem Fall werden die Administrationsagenten auf den Geräten im Remote-Büro (zwecks Synchronisierung) nicht direkt, sondern über ein Gateway mit dem Administrationsserver verbunden.

Da der Administrationsserver das Netzwerk im Remote-Büro aller Wahrscheinlichkeit nach nicht abfragen kann, ist es sinnvoll, das Ausführen dieser Funktion auf einen der Verteilungspunkte zu übertragen.

Der Administrationsserver kann an verwaltete Geräte, welche sich im Remote-Büro hinter NAT befinden, keine Benachrichtigung an den UDP-Port 15000 senden. Um dieses Problem zu beheben, können Sie in den Eigenschaften der Geräte, die als Verteilungspunkte dienen, den Modus zur ständigen Verbindung mit dem Administrationsserver (Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen**) aktivieren. Dieser Modus ist verfügbar, wenn die Gesamtanzahl der Verteilungspunkte 300 nicht überschreitet. Verwenden Sie Push-Server, um sicherzustellen, dass eine kontinuierliche Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver besteht. Weitere Informationen finden Sie in dem folgenden Artikel: Einen Push-Server aktivieren.

Struktur des Schutzes im Unternehmen auswählen

Die Auswahl einer Struktur für den Schutz im Unternehmen wird durch folgende Faktoren bestimmt:

- Netztopologie des Unternehmens
- Organisationsstruktur
- Anzahl der für den Antiviren-Schutz zuständigen Mitarbeiter und deren Aufgabenverteilung
- Hardwareressourcen, die für die Installation von Antiviren-Schutzkomponenten zur Verfügung gestellt werden können
- Bandbreite der Kommunikationskanäle, die für den Einsatz der Antiviren-Schutzkomponenten im Netzwerk des Unternehmens zur Verfügung gestellt werden können
- Annehmbare Zeit für die Durchführung von kritischen administrativen Vorgängen im Netzwerk des Unternehmens Zu kritischen administrativen Vorgängen gehören zum Beispiel die Verbreitung von Updates der Antiviren-Datenbanken und die Veränderung von Richtlinien für die Client-Geräte

Bei der Wahl der Antiviren-Schutzstruktur empfiehlt es sich, zunächst die vorhandenen Netzwerk- und Hardwareressourcen zu bestimmen, die sich für das zentrale Virenschutz-System verwenden lassen.

Für die Analyse der Netzwerk- und Hardwareinfrastruktur wird die folgende Vorgehensweise empfohlen:

1. Legen Sie die folgenden Einstellungen für das Netzwerk fest, in dem die Antiviren-Programme verteilt werden sollen:

   - Anzahl der Netzwerksegmente.
   - Geschwindigkeit der Kommunikationskanäle zwischen den einzelnen Netzwerksegmenten.
   - Anzahl der verwalteten Geräte in jedem Netzwerksegment.
   - Bandbreite aller Kommunikationskanäle, die für den Antiviren-Schutz zur Verfügung gestellt werden kann.

2. Definieren Sie die zulässige Dauer für die Durchführung wichtiger administrativer Operationen für alle verwalteten Geräte.

3. Analyse der Informationen aus den Punkten 1 und 2, sowie der Daten der Belastungstests des Administrationssystems. Beantworten Sie anhand der durchgeführten Analyse folgende Fragen:

   - Können alle Clients mit einem einzigen Administrationsserver bedient werden oder ist eine Hierarchie von Administrationsservern erforderlich?
   - Welche Hardwarekonfiguration der Administrationsserver ist nötig, um alle Clients in der in Punkt 2 festgelegten Zeit zu bedienen?
   - Ist eine Verwendung von Verteilungspunkten nötig, um die Auslastung der Kommunikationskanäle zu verringern?

Nachdem Sie die oben in Punkt 3 angeführten Fragen beantwortet haben, können Sie denkbare Antiviren-Schutzstrukturen für das Unternehmen zusammenstellen.

Im Netzwerk des Unternehmens kann eine der folgenden typischen Antiviren-Schutzstrukturen verwendet werden:

- Ein einziger Administrationsserver. Alle Client-Geräte sind mit einem einzigen Administrationsserver verbunden. Der Administrationsserver agiert als Verteilungspunkt.
- Ein einziger Administrationsserver mit Verteilungspunkten. Alle Client-Geräte sind mit einem einzigen Administrationsserver verbunden. Im Netzwerk sind Client-Geräte zur Verfügung gestellt, die als Verteilungspunkte agieren.
- Administrationsserver-Hierarchie. Für jedes Netzwerksegment wird ein separater Administrationsserver zur Verfügung gestellt, der in die allgemeine Hierarchie der Administrationsserver eingeschlossen ist. Der primäre Administrationsserver agiert als Verteilungspunkt.
- Administrationsserver-Hierarchie mit Verteilungspunkten. Für jedes Netzwerksegment wird ein separater Administrationsserver zur Verfügung gestellt, der in die allgemeine Hierarchie der Administrationsserver eingeschlossen ist. Im Netzwerk sind Client-Geräte zur Verfügung gestellt, die als Verteilungspunkte agieren.

Typische Vorgehensweisen der Bereitstellung

In diesem Abschnitt werden typische Methoden zur Bereitstellung des Schutzsystems mithilfe von Kaspersky Security Center in einem Unternehmensnetzwerk beschrieben.

Das System muss vor unbefugten Zugriffen aller Art geschützt werden. Es wird empfohlen, vor der Installation des Programms auf Ihrem Gerät alle verfügbaren Updates des Betriebssystems zu installieren und die Administrationsserver sowie die Verteilungspunkte vor physischem Zugriff zu schützen.

Sie können Antiviren-Programme im Netzwerk eines Unternehmens mithilfe von Kaspersky Security Center bereitstellen, indem Sie folgende Vorgehensweisen zur Bereitstellung verwenden:

- Bereitstellung eines Schutzsystems über Kaspersky Security Center Web Console.

  Die Installation von Kaspersky-Anwendungen auf Client-Geräten und die Verbindung von Client-Geräten mit dem Administrationsserver erfolgt automatisch mithilfe von Kaspersky Security Center.

- Manuelle Bereitstellung der Antiviren-Programme mithilfe autonomer Installationspakete, die in Kaspersky Security Center erstellt wurden

  Die Installation von Kaspersky-Anwendungen auf den Client-Geräten und dem Administrator-Arbeitsplatz erfolgt manuell. Die Einstellungen für die Verbindung der Client-Geräte mit dem Administrationsserver werden bei der Installation des Administrationsagenten vorgegeben.

  Diese Variante der Bereitstellungwird empfohlen, wenn keine Remote-Installation möglich ist.

Kaspersky Security Center unterstützt keine Bereitstellung mithilfe der Gruppenrichtlinien des Microsoft Active Directory®.

Auswahl des DBMS

In der nachfolgenden Tabelle sind die zulässigen DBMS-Varianten und deren Empfehlungen und Einschränkungen zur Verwendung aufgeführt.

Empfehlungen und Einschränkungen der DBMSs

DBMS	Empfehlungen und Einschränkungen
MySQL (siehe unterstützte Versionen)	Verwenden Sie dieses DBMS, wenn Sie einen Administrationsserver für bis zu 20.000 Geräte verwenden möchten.
MariaDB (siehe unterstützte Versionen)	Verwenden Sie dieses DBMS, wenn Sie einen Administrationsserver für bis zu 20.000 Geräte verwenden möchten.
PostgreSQL, Postgres Pro (siehe unterstützte Versionen)	Verwenden Sie dieses DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 50.000 Geräte einzusetzen.
Tantor (siehe unterstützte Versionen)	Verwenden Sie dieses DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 50.000 Geräte einzusetzen. Das Tantor-DBMS wird nur von Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.8) unterstützt.

Informationen zur Installation des ausgewählten DBMS finden Sie in der DBMS-Dokumentation.

Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren.

Wenn Sie sich entscheiden, PostgreSQL oder Postgres Pro als DBMS zu installieren, stellen Sie sicher, dass Sie ein Kennwort für den Superuser angegeben haben. Wenn das Kennwort nicht angegeben wird, kann sich der Administrationsserver möglicherweise nicht mit der Datenbank verbinden.

Wenn Sie MySQL, MariaDB, PostgreSQL, oder Postgres Pro installieren, verwenden Sie die empfohlenen Einstellungen, um sicherzustellen, dass das DBMS ordnungsgemäß funktioniert.

Wenn Sie PostgreSQL, MariaDB oder MySQL als DBMS verwenden, wird auf der Registerkarte **Ereignisse** möglicherweise eine unvollständige Liste der Ereignisse für das ausgewählte Client-Gerät angezeigt. Dies kommt vor, wenn das DBMS eine sehr große Anzahl von Ereignissen speichert. Sie können die Anzahl der angezeigten Ereignisse auf eine der folgenden Arten erhöhen:

- Nicht benötigte Ereignisse entfernen.
- Speicherdauer für nicht benötigte Ereignisse verkürzen.

Verwenden Sie die Berichte, um eine vollständige Liste der auf dem Administrationsserver für das Gerät protokollierten Ereignisse anzuzeigen.

Internetzugriff für den Administrationsserver bereitstellen

Für die folgenden Fälle muss der Zugriff auf den Administrationsserver aus dem Internet gewährt werden:

- Regelmäßiges Aktualisieren der Datenbanken, Softwaremodule und Programme von Kaspersky
- Aktualisieren von Drittanbieter-Programmen

  Standardmäßig ist für den Administrationsserver keine Internetverbindung erforderlich, um Updates für Software von Microsoft auf den verwalteten Geräten zu installieren. Beispielsweise können die verwalteten Geräte die Updates für Software von Microsoft direkt von den Microsoft Update-Servern oder von einem Windows Server mit im Unternehmensnetzwerk bereitgestelltem Microsoft Windows Server Update Services (WSUS) herunterladen. In den folgenden Fällen muss der Administrationsserver mit dem Internet verbunden sein:

  - Wenn Sie Administrationsserver als WSUS-Server verwenden
  - So installieren Sie Updates für Drittanbieter-Programme, die keine Software von Microsoft darstellen
- Schließen von Schwachstellen in Programmen von Drittanbietern

  Damit der Administrationsserver die folgenden Aufgaben ausführen kann, ist eine Internetverbindung erforderlich:

  - Erstellen einer Liste empfohlener Korrekturen für Schwachstellen in Software von Microsoft. Die Liste wird von Kaspersky-Spezialisten erstellt und regelmäßig aktualisiert.
  - Schwachstellen Drittanbieter-Programmen beheben, keine Software von Microsoft darstellen.
- Für die Verwaltung von Geräten (Laptops) der eigenständigen Benutzer

- Für die Verwaltung von Geräten, die sich in Remote-Büros befinden
- Bei der Interaktion mit primären oder sekundären Administrationsservern, die sich in Remote-Büros befinden
- Zur Verwaltung von mobilen Geräten

In diesem Abschnitt werden die typischen Methoden zur Gewährleistung des Zugriffs auf den Administrationsserver über das Internet beschrieben. Für alle Fälle der Bereitstellung des Zugriffes auf den Administrationsserver über das Internet kann es erforderlich sein, für den Administrationsserver ein spezielles Zertifikat festzulegen.

Internetzugriff: Administrationsserver in einem lokalen Netzwerk

Wenn sich der Administrationsserver im internen Netzwerk eines Unternehmens befindet, kann es hilfreich sein, den TCP-Port 13000 des Administrationsservers mithilfe der Portweiterleitung von außen erreichbar zu machen.

Zugriff aus dem Internet: Administrationsserver in der demilitarisierten Zone

Wenn sich der Administrationsserver in der demilitarisierten Zone eines Unternehmensnetzwerks befindet, hat er keinen Zugriff auf das interne Netzwerk des Unternehmens. Daraus ergeben sich die folgenden Einschränkungen:

- Der Administrationsserver kann neue Geräte nicht selbstständig finden.
- Der Administrationsserver kann die erstmalige Bereitstellung des Administrationsagenten nicht mittels erzwungener Installation auf den Geräten des internen Netzwerks des Unternehmens ausführen.

  Es handelt sich nur um die erstmalige Installation des Administrationsagenten. Die nachfolgenden Updates der Version des Administrationsagenten oder die Installation der Sicherheitsanwendungen können bereits vom Administrationsserver ausgeführt werden.

Beachten Sie, dass Kaspersky Security Center Linux die Bereitstellung mithilfe von Gruppenrichtlinien von Microsoft Windows nicht unterstützt.

Sie können Verteilungspunkte verwenden, die sich im Unternehmensnetzwerk befinden. Für das Ausführen der erstmaligen Bereitstellung auf Geräten ohne Administrationsagenten muss der Administrationsagent vorläufig auf einem der Geräte installiert und dieses Gerät als Verteilungspunkt bestimmt werden. Daraufhin wird die erstmalige Installation des Administrationsagenten auf den übrigen Geräten vom Administrationsserver durch diesen Verteilungspunkt ausgeführt.

Um sicherzustellen, dass Benachrichtigungen an den UDP-Port 15000 erfolgreich auf verwalteten Geräten gesendet werden, die sich im internen Unternehmensnetzwerk befinden, müssen Sie das gesamte Unternehmensnetzwerk mit Verteilungspunkten abdecken. Aktivieren Sie in den Eigenschaften der zugewiesenen Verteilungspunkte das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen**. Dadurch stellt der Administrationsserver eine kontinuierliche Verbindung zu den Verteilungspunkten her und die Verteilungspunkte können Benachrichtigungen an den UDP-Port 15000 auf den Geräten senden, die sich im internen Unternehmensnetzwerk befinden (das trifft auf IPv4- oder IPv6-Netzwerke zu).

Installation

Dieser Abschnitt beschreibt die Installation für Kaspersky Security Center Linux und Kaspersky Security Center Web Console.

Den MariaDB x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren

Um den Server von MariaDB x64 erfolgreich für die Arbeit mit Kaspersky Security Center zu konfigurieren, müssen Sie mit Ausnahme der in diesem Artikel angegebenen Serverparameter die standardmäßigen Serverparameter verwenden.

Empfohlene Einstellungen für die Datei my.cnf

Weitere Informationen zur Konfiguration des DBMS finden Sie auch in der Vorgehensweise zur Konfiguration von Benutzerkonten. Weitere Informationen zur Installation des DBMS finden Sie in der Vorgehensweise zur Installation eines DBMS.

Um die Datei my.cnf zu konfigurieren:

1. Öffnen Sie die Datei my.cnf in einem Texteditor.

2. Geben Sie in der Datei "my.cnf" im Abschnitt [mysqld] die folgenden Zeilen ein:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=<der tatsächliche Wert muss nicht weniger als 80 % der Größe
der erwarteten KAV-Datenbank sein>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

   Der Wert von `innodb_buffer_pool_size` muss mindestens 80 Prozent der erwarteten KAV-Datenbankgröße betragen. Beachten Sie, dass der angegebene Speicher beim Start des Servers zugewiesen wird. Wenn die Datenbankgröße kleiner als der angegebene Buffer-Wert ist, wird nur der erforderliche Speicher zugewiesen. Wenn Sie MariaDB 10.4.3 oder älter verwenden, ist die tatsächliche Größe des zugewiesenen Speichers etwa 10 Prozent größer als der angegebene Buffer-Wert.

Es wird empfohlen, den Parameterwert `innodb_flush_log_at_trx_commit=0` zu verwenden, da die Werte "1" oder "2" die Geschwindigkeit von MariaDB negativ beeinflussen. Stellen Sie sicher, dass der Parameter `innodb_file_per_table` auf `1` gesetzt ist.

Geben Sie für MariaDB 10.1 zusätzlich die folgenden Zeilen im "[mysqld]"-Abschnitt ein:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

Geben Sie für MariaDB 10.6 zusätzlich die folgenden Zeilen im "[mysqld]"-Abschnitt ein:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Standardmäßig sind die Optimierungs-Add-ons `join_cache_incremental`, `join_cache_hashed` und `join_cache_bka` aktiviert. Wenn diese Add-ons nicht aktiviert sind, müssen Sie diese aktivieren.

Um zu überprüfen, ob die Optimierungs-Add-ons aktiviert sind:

1. Führen Sie in der MariaDB-Client-Konsole den folgenden Befehl aus:

   ```
   SELECT @@optimizer_switch;
   ```

2. Stellen Sie sicher, dass die Ausgabe die folgenden Zeilen enthält:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Wenn diese Zeilen vorhanden sind und die Werte `on` haben, sind die Optimierungs-Add-ons aktiviert.

   Falls diese Zeilen fehlen oder die Werte `off` haben:

   a. Öffnen Sie die Datei my.cnf in einem Texteditor.

   b. Fügen Sie die folgenden Zeilen in die Datei my.cnf ein:

   ```
   optimizer_switch='join_cache_incremental=on'
   optimizer_switch='join_cache_hashed=on'
   optimizer_switch='join_cache_bka=on'
   ```

Die Add-ons `join_cache_incremental`, `join_cache_hash` und `join_cache_bka` sind aktiviert.

Erhöhen Sie für den systemd-Dienst von MariaDB die Obergrenze für Dateien, die geöffnet werden können (Dateideskriptoren), um bei hoher Auslastung Stabilität zu gewährleisten.

So erhöhen Sie die Obergrenze der Dateideskriptoren:

1. Führen Sie den folgenden Befehl aus:

   ```
   sudo systemctl edit mariadb.service
   ```

2. Geben Sie die Obergrenze der Dateideskriptoren im Parameter `LimitNOFILE` des Abschnitts `[Service]` an:

   ```
   LimitNOFILE=1048576
   ```

3. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Parameter korrekt angegeben wurden:

   ```
   sudo systemd-analyze verify mariadb.service
   ```

4. Führen Sie den folgenden Befehl aus, um den Prozess "systemd" neu zu laden:

   ```
   sudo systemctl daemon-reload
   ```

5. Führen Sie den folgenden Befehl aus, um den Dienst von MariaDB neu zu starten:

   `sudo systemctl restart mariadb.service`

   Die Obergrenze der Dateideskriptoren wurde erhöht.

PostgreSQL- oder Postgres Pro-Server für die Ausführung mit Kaspersky Security Center Linux konfigurieren

Um den Server von PostgreSQL oder Postgres Pro erfolgreich für die Arbeit mit Kaspersky Security Center Linux einzurichten, müssen Sie mit Ausnahme der in diesem Artikel angegebenen Serverparameter die standardmäßigen Serverparameter verwenden.

Kaspersky Security Center Linux unterstützt PostgreSQL und Postgres Pro als DBMS. Wenn Sie eines dieser DBMS verwenden, sollten Sie die Parameter des entsprechenden DBMS-Servers konfigurieren, um die Ausführung des DBMS in Bezug auf Kaspersky Security Center Linux zu optimieren.

Der Standardpfad zur Konfigurationsdatei lautet: `/etc/postgresql/<VERSION>/main/postgresql.conf`

Unter dem Betriebssystem Linux ALT lautet der Standardpfad `/var/lib/pgsql/data/postgresql.conf`

Empfohlene Parameter für PostgreSQL und Postgres Pro:

- `max_connections = 151`

  Wenn Sie ein DBMS-Cluster unter Postgres verwenden, geben Sie für alle DBMS-Server sowie in der Cluster-Konfiguration den Parameter `max_connections` an.

- `shared_buffers` = N

  N = 25% der geschätzten RAM-Größe für das DBMS. Wenn das DBMS auf einem Gerät zusammen mit dem Administrationsserver installiert ist, sollte die Berechnung auf dem für das DBMS reservierten RAM basieren, nicht auf dem gesamten RAM des Geräts.

  Wenn der Arbeitsspeicher weniger als 1 GB beträgt, belassen Sie den Standardwert.

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `maintenance_work_mem = 128MB`

- `max_stack_depth` = maximale Stapelgröße (führen Sie den Befehl `ulimit -s` aus, um diesen Wert in KB zu erhalten) minus 1 MB Sicherheitsdifferenz

- `max_parallel_workers_per_gather = 0`

- `standard_conforming_strings` = `on`

Wenn Sie Postgres Pro 15.7 oder Postgres Pro 15.7.1 verwenden, deaktivieren Sie den Parameter `enable_compound_index_stats`:

```
enable_compound_index_stats = off
```

Laden Sie die Konfiguration neu oder starten Sie den DBMS-Server neu, nachdem Sie die Konfigurationsdatei aktualisiert haben.

Weitere Informationen zu den Serverparametern von PostgreSQL und Postgres Pro und zu deren Konfiguration finden Sie in der entsprechenden DBMS-Dokumentation.

Weitere Informationen zum Erstellen und Konfigurieren von Konten für PostgreSQL und Postgres Pro finden Sie im folgenden Artikel: Benutzerkonten für die Arbeit mit PostgreSQL und Postgres Pro konfigurieren.

Weitere Informationen zur Konfiguration einem hochverfügbaren DBMS-Clusters erhalten Sie in diesem Artikel: Ein hochverfügbares DBMS-Cluster für die Arbeit mit Kaspersky Security Center Linux vorbereiten.

Den MySQL x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren

Um den Server von MySQL x64 erfolgreich für die Arbeit mit Kaspersky Security Center einzurichten, müssen Sie mit Ausnahme der in diesem Artikel angegebenen Serverparameter die standardmäßigen Serverparameter verwenden.

Wenn Sie den MySQL-Server für Kaspersky Security Center verwenden, aktivieren Sie die Unterstützung für InnoDB und MEMORY-Speicher sowie für die Codierungen UTF-8 und UCS-2.

Empfohlene Einstellungen für die Datei my.cnf

Weitere Informationen zur Konfiguration des DBMS finden Sie auch in der Vorgehensweise zur Konfiguration von Benutzerkonten. Weitere Informationen zur Installation des DBMS finden Sie in der Vorgehensweise zur Installation eines DBMS.

Um die Datei my.cnf zu konfigurieren:

1. Öffnen Sie die Datei my.cnf in einem Texteditor.

2. Fügen Sie der Datei "my.cnf" im Abschnitt `[mysqld]` die folgenden Zeilen hinzu:

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=<der tatsächliche Wert muss nicht weniger als 80 % der Größe der erwarteten KAV-Datenbank sein>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (in den meisten Fällen nutzt der Server kleine Transaktionen)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
```

```
table_open_cache_instances=4
table_definition_cache=60000
```

Beachten Sie, dass der für den Wert `innodb_buffer_pool_size` angegebene Speicher beim Start des Servers zugewiesen wird. Wenn die Datenbankgröße kleiner als der angegebene Buffer-Wert ist, wird nur der erforderliche Speicher zugewiesen. Die tatsächliche Größe des zugewiesenen Speichers ist ungefähr 10 Prozent größer als der angegebene Buffer-Wert. Weitere Informationen entnehmen Sie der Dokumentation zu MySQL.

Es wird empfohlen, den Parameterwert `innodb_flush_log_at_trx_commit = 0` zu verwenden, da die Werte "1" oder "2" die Geschwindigkeit von MySQL negativ beeinflussen. Stellen Sie sicher, dass der Parameter `innodb_file_per_table` auf `1` gesetzt ist.

Ein hochverfügbares DBMS-Cluster für die Arbeit mit Kaspersky Security Center Linux vorbereiten

Kaspersky Security Center Linux unterstützt die folgenden hochverfügbaren Cluster:

- Platform V Pangolin
- Postgres Pro Built-in High Availability
- Patroni (mit optionalem HAProxy Load Balancer)

Der Replikationstyp muss auf "synchron" eingestellt sein.

Wenn Sie für PostgreSQL das Patroni-Template Version 3.3.1 oder früher verwenden, stellen Sie sicher, dass der Parameter `synchronous_standby_names` korrekt angewendet wird. Um zu überprüfen, dass die synchrone Replikation verwendet wird, führen Sie die folgende Abfrage auf dem primären Knoten aus:

```
SELECT application_name, client_addr, client_hostname, client_port, sync_state
FROM pg_stat_replication;
```

Wenn in der Spalte `sync_state` für einen beliebigen Knoten Werte angezeigt werden, die von `sync` oder `potential` abweichen, verwendet das Cluster die asynchrone Replikation. Diese wird nicht unterstützt. Führen Sie einen der folgenden Schritte aus, um dieses Problem zu beheben:

- Aktualisieren Sie Patroni auf Version 3.3.2 oder höher.
- Suchen Sie in der Konfigurationsdatei für Patroni im Abschnitt `bootstrap` den Unterabschnitt `dcs` und setzen Sie den Parameter `synchronous_mode` auf `true`:

  `bootstrap:`

  `dcs:`

  `<...>`

  `synchronous_mode: true`

Die empfohlene Konfiguration für ein minimales, hochverfügbares DBMS-Cluster muss mindestens drei Knoten umfassen:

So bereiten Sie ein hochverfügbares DBMS-Cluster für die Arbeit mit Kaspersky Security Center Linux vor:

1. PostgreSQL- oder Postgres Pro-Server für die Ausführung mit Kaspersky Security Center Linux konfigurieren.

2. Wenn Sie möchten, dass der Administrationsserver alle Adressen der Cluster-Knoten automatisch erkennt, damit Sie während der Installation ausschließlich den DNS-Namen oder die IP-Adresse des primären Knotens oder des Replika-Knotens angeben müssen, führen Sie folgende Schritte aus:

   a. Ändern Sie auf allen Knoten des hochverfügbaren DBMS-Clusters die Konfigurationsdatei "/etc/pangolin-manager/postgres.yml" (wenn Sie Platform V Pangolin verwenden) oder "/etc/postgresql/<VERSION>/main/postgresql.conf" (wenn Sie ein Cluster von Postgres Pro Built-in High Availability verwenden), indem Sie dem Abschnitt `postgresql` folgende Zeile hinzufügen:

   `log_hostname=1`

   Für die sonstigen Parameter der Konfigurationsdatei können Sie die für PostgreSQL und Postgres Pro empfohlenen Werte verwenden.

   b. Starten Sie nach dem Ändern der Konfigurationsdatei den Dienst des DBMS-Clusters auf allen hochverfügbaren Cluster-Knoten neu.

   c. Stellen Sie sicher, dass der Datenbankbenutzer die Berechtigung `pg_read_all_stats` besitzt. Sie können diese Berechtigung erteilen, indem Sie den folgenden Befehl ausführen:

   `GRANT pg_read_all_stats TO "%1";`

   Wobei `%1` für den Namen des Datenbankbenutzers steht.

   Der Benutzername wird während der Installation des Administrationsservers im Parameter `KLSRV_UNATT_DBMS_LOGIN` angegeben.

   d. Konfigurieren Sie den Load Balancer für die IAM-Datenbank. Informationen dazu entnehmen Sie der Dokumentation des von Ihnen gewählten Load Balancers.

Das hochverfügbare DBMS-Cluster ist bereit für die Arbeit mit Kaspersky Security Center Linux.

Kaspersky Security Center Linux installieren

In diesem Ablauf wird beschrieben, wie Kaspersky Security Center Linux installiert wird.

Folgende Schritte müssen Sie vor der Installation ausführen:

- Installieren Sie das DBMS für die Verwendung mit Kaspersky Security Center Linux Sie können eins der unterstützten DBMS verwenden. Informationen zur Installation des ausgewählten DBMS finden Sie in dessen Dokumentation.

  Wenn die Distribution Ihres Linux-basierten Betriebssystems ohne unterstütztes DBMS ausgeliefert wird, können Sie das DBMS aus der Paketverwaltung eines Drittanbieters installieren.

Folgen Sie nach der Installation des DBMS der entsprechenden Anweisung:

- PostgreSQL- oder Postgres Pro-Server für die Ausführung mit Kaspersky Security Center Linux konfigurieren

  DBMS-Benutzerkonto für die Arbeit mit PostgreSQL und Postgres Pro konfigurieren

  Wenn Sie möchten, dass der Administrationsserver die Adressen der Cluster-Knoten automatisch erkennt, damit Sie während der Installation nur den DNS-Namen oder die IP-Adresse des primären Knotens oder des Replika-Knotens angeben müssen, vergewissern Sie sich, dass Sie Schritt 2 der Anweisung im folgenden Artikel ausgeführt haben: Ein hochverfügbares DBMS-Cluster für die Arbeit mit Kaspersky Security Center Linux vorbereiten.

- Den MariaDB x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren

  DBMS-Benutzerkonto für die Arbeit mit MySQL und MariaDB konfigurieren

- Den MySQL x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren

  DBMS-Benutzerkonto für die Arbeit mit MySQL und MariaDB konfigurieren

- Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center Linux installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

  Wenn Sie das Betriebssystem RED OS 7.3.4 und höher bzw. MSVSPHERE 9.2 und höher verwenden, installieren Sie das Paket "libxcrypt-compat", damit der Administrationsserver funktioniert wie vorgesehen.

- Stellen Sie sicher, dass der DNS-Server im Netzwerk verfügbar ist.

- Laden Sie die Installationsdatei von der Kaspersky-Website herunter. Wählen Sie die Installationsdatei aus, die der auf Ihrem Gerät installierten Linux-Distribution entspricht: ksc64_[Versionsnummer]_amd64.deb oder ksc64-[Versionsnummer].x86_64.rpm.

Um Kaspersky Security Center Linux zu installieren, müssen Sie die in den folgenden Schritten angegebenen Befehle unter einem Benutzerkonto mit Root-Rechten ausführen.

So installieren Sie Kaspersky Security Center Linux:

1. Erstellen Sie die Gruppe "kladmins" und die nicht-privilegierten Konten "ksc" und "ksciam". Das Benutzerkonto muss Mitglied der Gruppe "kladmins" sein. Führen Sie dazu nacheinander die folgenden Befehle aus:

   ```
   adduser ksc
   ```

   ```
   groupadd kladmins
   ```

   ```
   gpasswd -a ksc kladmins
   ```

   ```
   usermod -g kladmins ksc
   ```

   ```
   adduser ksciam
   ```

   ```
   gpasswd -a ksciam kladmins
   ```

   ```
   usermod -g kladmins ksciam
   ```

2. Erstellen Sie auf dem DBMS-Server eine Datenbank für IAM. Der Name der Datenbank muss sich von dem Namen der Datenbank unterscheiden, die Sie zur Verwendung mit Kaspersky Security Center Linux installiert haben. Der Administrationsserver löscht die IAM-Datenbank nicht automatisch, wenn der Server deinstalliert oder auf ein anderes Gerät verschoben wird. Sie müssen die Datenbank manuell entfernen.

   - Für PostgreSQL führen Sie den folgenden Befehl aus:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
     ```

   - Für MariaDB führen Sie den folgenden Befehl aus:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
     ```

3. Wenn Sie ein hochverfügbares DBMS-Cluster verwenden, führen Sie die folgenden Schritte aus:

   a. Gewähren Sie dem Benutzer "ksc" die Berechtigung `pg_read_all_stats`:

   ```
   GRANT pg_read_all_stats TO "ksc";
   ```

   b. Ändern Sie auf allen Knoten des hochverfügbaren DBMS-Clusters die Konfigurationsdatei "/etc/pangolin-manager/postgres.yml" (wenn Sie Platform V Pangolin verwenden) oder "/etc/postgresql/main/postgresql.conf" (wenn Sie ein Cluster von Postgres Pro Built-in High Availability verwenden). Fügen Sie dem Abschnitt `postgresql` die folgende Zeile hinzu, wenn Sie beim Verbinden des Clusters mit Kaspersky Security Center Linux nur den DNS-Namen oder die IP-Adresse des primären Knotens oder Replika-Knotens angeben möchten:

   ```
   log_hostname: '1'
   ```

   c. Starten Sie nach dem Ändern der Konfigurationsdatei "/etc/pangolin-manager/postgres.yml" den Dienst des DBMS-Clusters auf allen hochverfügbaren Cluster-Knoten (mit Ausnahme des Vermittler-Knotens) neu.

   ```
   systemctl restart pangolin-manager.service
   ```

   oder

   ```
   systemctl restart postgresql-<version>
   ```

4. Erhöhen Sie bei Bedarf für die Benutzerkonten, die für die Funktionen des Administrationsservers verwendet werden, die Anzahl an Dateien, die standardmäßig geöffnet werden können (Datei-Deskriptoren). Öffnen Sie dazu die Datei "/etc/security/limits.conf" und geben Sie die weichen und harten Beschränkungen der Datei-Deskriptoren wie folgt an:

   ```
   ksc  soft  nofile  <max_number_of_opened_files>
   ```

   ```
   ksc  hard  nofile  <max_number_of_opened_files>
   ```

   Standardmäßig werden die Limits der Datei-Deskriptoren während der Installation angegeben. Die das weiche Datei-Limit beträgt 32.768 und das harte Datei-Limit 131.072 Dateien.

5. Führen Sie die Installation von Kaspersky Security Center Linux aus. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

```
sudo yum install /<path>/ksc64-<version_number>.x86_64.rpm
```

6. Führen Sie die Konfiguration von Kaspersky Security Center Linux aus:

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

7. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA) und die Datenschutzrichtlinie. Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie nach der entsprechenden Aufforderung die folgenden Werte ein:

   a. Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren. Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der EULA zustimmen.

   b. Geben Sie `y` ein, wenn Sie die Bedingungen der Datenschutzrichtlinie verstehen und akzeptieren, und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Geben Sie `n` ein, wenn Sie den Bedingungen der Datenschutzrichtlinie nicht zustimmen. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der Datenschutzrichtlinie zustimmen.

8. Geben Sie nach der entsprechenden Aufforderung die folgenden Einstellungen ein:

   a. Wählen Sie **Standard** als Installationsmodus des Administrationsservers aus.

   b. Geben Sie den DNS-Namen oder die statische IP-Adresse des Administrationsservers ein. Diese Adresse wird von anderen Geräten für die Verbindung mit dem Administrationsserver verwendet.

   c. Geben Sie die SSL-Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 13000 festgelegt.

   d. Ermitteln Sie die ungefähre Anzahl der Geräte, die Sie verwalten möchten:

      - Geben Sie für 1 bis 100 verwaltete Geräte den Wert 1 ein.
      - Geben Sie für 101 bis 1.000 verwaltete Geräte den Wert 2 ein.
      - Geben Sie für über 1.000 verwaltete Geräte den Wert 3 ein.

      Diese Einstellung dient der automatischen, zufälligen Verzögerung von Aufgabenstarts, um die Auslastung auf das Netzwerk zu optimieren. Die folgende Liste enthält die Intervalle, innerhalb denen die Verzögerung berechnet wird:

      - 1 bis 100 verwaltete Geräte, Wert 1. Es wird keine Verzögerung verwendet.
      - 101 bis 1.000 verwaltete Geräte, Wert 2. Die Verzögerung beträgt 5 Minuten.
      - Über 1.000 verwaltete Geräte, Wert 3. Die Verzögerung beträgt 10 Minuten.

e. Geben Sie den Namen der Sicherheitsgruppe für Dienste ein. Standardmäßig wird die Gruppe `kladmins` verwendet.

f. Geben Sie den Namen des Benutzerkontos ein, um den Administrationsserver-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto `ksc` verwendet.

g. Geben Sie den Namen des Benutzerkontos ein, um andere Dienste zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto `ksc` verwendet.

h. Wählen Sie das DBMS aus, das Sie für die Verwendung mit Kaspersky Security Center Linux installiert haben:

- Wenn Sie MySQL oder MariaDB installiert haben, geben Sie "1" ein.
- Wenn Sie PostgreSQL oder Postgres Pro installiert haben, geben Sie "2" ein.

i. Geben Sie den DNS-Namen oder die IP-Adresse des Geräts ein, auf dem die Datenbank des Administrationsservers installiert ist (für eine lokale DBMS-Installation standardmäßig 127.0.0.1).

Um ein hochverfügbares Failover-Cluster zu verwenden, gehen Sie wie folgt vor:

- Geben Sie für alle Knoten die DNS-Namen oder IP-Adressen und Ports im folgenden Format ein:

```
<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
```

- Geben Sie nur den DNS-Namen oder die IP-Adresse des primären Knotens oder Replika-Knotens an.

j. Geben Sie die Portnummer der Datenbank ein. Dieser Port wird für die Kommunikation mit dem Administrationsserver verwendet. Dieser Schritt wird übersprungen, wenn Sie in Schritt 8.h die DNS-Namen oder IP-Adressen und Ports aller hochverfügbaren Cluster-Knoten angegeben haben.

Standardmäßig werden die folgenden Ports verwendet:

- Port `3306` für MySQL oder MariaDB
- Port `5432` für PostgreSQL oder Postgres Pro

k. Geben Sie den Namen der Datenbank ein.

l. Geben Sie den Benutzernamen für das Konto des Datenbank-Administrators ein, das Sie für den Zugriff auf die Datenbank verwenden.

m. Geben Sie das Kennwort für das Konto des Datenbank-Administrators ein, das Sie für den Zugriff auf die Datenbank verwenden.

n. Wenn Sie PostgreSQL oder Postgres Pro installiert haben, können Sie das Datenbankschema angeben, das vom Administrationsserver verwendet werden soll. Geben Sie dazu den Namen des Schemas an.

> Beim Namen des Schemas muss die Groß- und Kleinschreibung beachtet werden: Sie dürfen nur Kleinbuchstaben verwenden.

Wenn Sie kein benutzerdefiniertes Schema verwenden möchten, drücken Sie die EINGABETASTE. Dadurch wird ein Standardschema verwendet.

o. Geben Sie den FQDN des IAM-Servers ein. Wenn Sie diese Variable nicht angeben, wird der DNS-Name von dem Gerät verwendet, auf dem der Administrationsserver installiert ist.

Sie müssen den DNS-Namen des Administrationsservers angeben, den Sie in Schritt 8a eingegeben haben.

p. Geben Sie den Namen des Kontos ein, um den IAM-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto "ksciam" verwendet.

q. Wählen Sie das DBMS aus, das Sie für die Verwendung des IAM-Dienstes installiert haben:

- Wenn Sie MySQL oder MariaDB installiert haben, geben Sie "1" ein.
- Wenn Sie PostgreSQL oder Postgres Pro installiert haben, geben Sie "2" ein.

r. Geben Sie die Adresse des IAM-DBMS ein, die der IAM-Dienst verwenden soll.

Um ein hochverfügbares Cluster zu verwenden, gehen Sie wie folgt vor:

- Geben Sie für alle Knoten die DNS-Namen oder IP-Adressen und Ports im folgenden Format ein:

```
<fqdn1>:<port>,<fqdn2>:<port>,<...><fqdnX>:<port>;
```

- Geben Sie nur den DNS-Namen oder die IP-Adresse des Load Balancers an.

s. Geben Sie die Portnummer des IAM-DBMS ein. Dieser Port wird für die Kommunikation mit dem IAM-Dienst verwendet. Dieser Schritt wird übersprungen, wenn Sie in Schritt 8.p die DNS-Namen oder IP-Adressen und Ports aller hochverfügbaren Cluster-Knoten angegeben haben.

Standardmäßig werden die folgenden Ports verwendet:

- Port 3306 für MySQL oder MariaDB
- Port 5432 für PostgreSQL oder Postgres Pro

t. Geben Sie den Namen der IAM-Datenbank ein, den der IAM-Dienst verwenden soll. Der Name der vom IAM-Dienst verwendeten Datenbank muss sich von der Datenbank unterscheiden, die vom Administrationsserver verwendet wird.

u. Geben Sie den Benutzernamen des Datenbank-Benutzerkontos ein, das Sie für den Zugriff auf die IAM-Datenbank verwenden.

v. Geben Sie das Kennwort des Datenbank-Benutzerkontos ein, das Sie für den Zugriff auf die IAM-Datenbank verwenden.

Warten Sie, bis die Dienste hinzugefügt und automatisch gestartet wurden:

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`
- `kliam_srv`

w. Wenn Sie PostgreSQL oder Postgres Pro installiert haben, können Sie das Datenbankschema, das von IAM verwendet werden soll, festlegen. Geben Sie dazu den Namen des Schemas an.

Wenn Sie kein benutzerdefiniertes Schema verwenden möchten, drücken Sie die EINGABETASTE. Dadurch wird ein Schema "public" verwendet.

> Beim Namen des Schemas wird die Groß- und Kleinschreibung berücksichtigt: Sie dürfen nur Kleinbuchstaben verwenden.
> Die folgenden Namen sind bereits von IAM reserviert und dürfen ebenfalls nicht angegeben werden: client, iam, ksc, locker, pat, scope, voltron.

x. Erstellen Sie ein Benutzerkonto, das als Administrator des Administrationsservers fungiert. Geben Sie den Benutzernamen und das Kennwort ein.

Das Kennwort muss den folgenden Regeln entsprechen:

- Das Benutzerkennwort muss mindestens 8 Zeichen und darf maximal 256 Zeichen enthalten.
- Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
  - Großbuchstaben (A–Z)
  - Kleinbuchstaben (a–z)
  - Ziffern (0–9)
  - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Wenn Sie diesen Schritt überspringen, können Sie einen neuen Benutzer später mit folgendem Befehl erstellen:

```
/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
```

Der Benutzer wird hinzugefügt und Kaspersky Security Center Linux wird installiert.

Installation des Administrationsagenten

Um das Gerät des Administrationsservers wie jedes andere verwaltete Gerät verwalten zu können, installieren Sie den Administrationsagenten für Linux auf dem Gerät des Administrationsservers. In diesem Fall wird der Administrationsagent für Linux installiert und funktioniert unabhängig von der Serverversion des Administrationsagenten, die Sie zusammen mit dem Administrationsserver installiert haben.

Überprüfung von Diensten

Verwenden Sie die folgenden Befehle, um zu überprüfen, ob ein Dienst ausgeführt wird oder nicht:

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`

- `systemctl status klwebsrv_srv.service`
- `systemctl status kliam_srv.service`

Kaspersky Security Center Linux im Silent-Modus installieren

Sie können Kaspersky Security Center Linux auf Linux-Geräten installieren, indem Sie eine Antwortdatei verwenden, um eine Installation im Silent-Modus auszuführen, d. h. ohne Benutzerbeteiligung. Die Antwortdatei enthält eine benutzerdefinierte Zusammenstellung von Installationsparametern: Variablen und ihre entsprechenden Werte.

Vor der Installation:

- Installieren Sie das DBMS für die Verwendung mit Kaspersky Security Center Linux Sie können eins der unterstützten DBMS verwenden. Informationen zur Installation des ausgewählten DBMS finden Sie in dessen Dokumentation.

  Wenn die Distribution Ihres Linux-basierten Betriebssystems ohne unterstütztes DBMS ausgeliefert wird, können Sie das DBMS aus der Paketverwaltung eines Drittanbieters installieren.

  Folgen Sie nach der Installation des DBMS der entsprechenden Anweisung:

  - PostgreSQL- oder Postgres Pro-Server für die Ausführung mit Kaspersky Security Center Linux konfigurieren

    DBMS-Benutzerkonto für die Arbeit mit PostgreSQL und Postgres Pro konfigurieren

    Wenn Sie möchten, dass der Administrationsserver die Adressen der Cluster-Knoten automatisch erkennt, damit Sie während der Installation nur den DNS-Namen oder die IP-Adresse des primären Knotens oder des Replika-Knotens angeben müssen, vergewissern Sie sich, dass Sie Schritt 2 der Anweisung im folgenden Artikel ausgeführt haben: Ein hochverfügbares DBMS-Cluster für die Arbeit mit Kaspersky Security Center Linux vorbereiten.

  - Den MariaDB x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren

    DBMS-Benutzerkonto für die Arbeit mit MySQL und MariaDB konfigurieren

  - Den MySQL x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren

    DBMS-Benutzerkonto für die Arbeit mit MySQL und MariaDB konfigurieren

- Stellen Sie sicher, dass auf Ihrem Gerät mit dem installierten DBMS keine DBMS-Benutzerkonten mit den folgenden Namen vorhanden sind:

  - client
  - iam
  - ksc
  - locker
  - pat
  - scope
  - voltron

- Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center Linux installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

  Wenn Sie das Betriebssystem RED OS 7.3.4 und höher bzw. MSVSPHERE 9.2 und höher verwenden, installieren Sie das Paket "libxcrypt-compat", damit der Administrationsserver funktioniert wie vorgesehen.

- Laden Sie die Installationsdatei von der Kaspersky-Website herunter. Wählen Sie die Installationsdatei aus, die der auf Ihrem Gerät installierten Linux-Distribution entspricht: ksc64_[Versionsnummer]_amd64.deb oder ksc64-[Versionsnummer].x86_64.rpm.

So installieren Kaspersky Security Center Linux im Silent-Modus:

1. Lesen Sie den Endbenutzer-Lizenzvertrag. Folgen Sie den unten aufgeführten Schritten nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.

2. Erstellen Sie eine Gruppe "kladmins" und die nicht-privilegierten Konten namens "ksc" und "ksciam", die Mitglieder der Gruppe "kladmins" sein müssen. Führen Sie dazu unter einem Benutzerkonto mit Root-Rechten nacheinander die folgenden Befehle aus:

   `adduser ksc`

   `groupadd kladmins`

   `gpasswd -a ksc kladmins`

   `usermod -g kladmins ksc`

   `adduser ksciam`

   `gpasswd -a ksciam kladmins`

   `usermod -g kladmins ksciam`

3. Erstellen Sie auf dem DBMS-Server eine Datenbank für IAM. Der Name der Datenbank muss sich von dem Namen der Datenbank unterscheiden, die Sie zur Verwendung mit Kaspersky Security Center Linux installiert haben. Der Administrationsserver löscht die IAM-Datenbank nicht automatisch, wenn der Server deinstalliert oder auf ein anderes Gerät verschoben wird. Sie müssen die Datenbank manuell entfernen.

   - Für PostgreSQL führen Sie den folgenden Befehl aus:

     `sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"`

   - Für MariaDB führen Sie den folgenden Befehl aus:

     `sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"`

4. Erstellen Sie die Antwortdatei (im txt-Format) und fügen Sie der Antwortdatei eine Liste mit Variablen im Format `VARIABLE_NAME=variable_value` hinzu. Verwenden Sie für jede Variable eine separate Zeile. Die Antwortdatei sollte die Variablen enthalten, die in der folgenden Tabelle aufgeführt sind.

5. Geben Sie in der root- oder Benutzerumgebung als Wert für die Umgebungsvariable `KLAUTOANSWERS` den vollständigen Namen der Antwortdatei, einschließlich des enthaltenen Pfades, mit dem folgenden Befehl an:

   `export KLAUTOANSWERS=/tmp/ksc_install/answers.txt`

6. Führen Sie die Installation von Kaspersky Security Center Linux im Silent-Modus aus. Verwenden Sie je nach Linux-Distribution einen der folgenden Befehle:

In der root-Umgebung:

- `apt-get install /<path>/ksc64_[Versionsnummer]_amd64.deb -y`
- `yum install /<path>/ksc64-[Versionsnummer].x86_64.rpm -y`

In der Benutzerumgebung:

- `sudo -E apt-get install /<path>/ksc64_[Versionsnummer]_amd64.deb -y`
- `sudo -E yum install /<path>/ksc64-[Versionsnummer].x86_64.rpm -y`

7. Legen Sie einen Benutzer für die Arbeit mit Kaspersky Security Center Web Console an. Führen Sie dazu den folgenden Befehl unter einem Benutzerkonto mit Root-Rechten aus:

   `/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <Kennwort>`, wobei das Kennwort mindestens 8 Zeichen enthalten muss.

8. Installieren Sie Kaspersky Security Center Web Console.

Verwendete Variablen der Antwort-Datei für die Installation von Kaspersky Security Center Linux im Silent-Modus

Name der Variablen	Erforderlich	Beschreibung	Mögliche Werte
`EULA_ACCEPTED`	Ja	Bestätigt, dass Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.	`1`
`PP_ACCEPTED`	Ja	Bestätigt, dass Sie die Bedingungen der Datenschutzrichtlinie verstehen und akzeptieren.	`1`
`KLSRV_UNATT_SERVERADDRESS`	Ja	Der DNS-Name oder die statische IP-Adresse des Administrationsservers.	DNS-Name oder IP-Adresse
`KLSRV_UNATT_PORT_SRV`	Nein	Die Portnummer des Administrationsservers. Optional. Standardwert ist 14000.	Portnummer
`KLSRV_UNATT_PORT_SRV_SSL`	Nein	Die SSL-Portnummer des Administrationsservers. Optional. Standardwert ist 13000.	Portnummer
`KLSRV_UNATT_PORT_KLOAPI`	Nein	Die Portnummer für die Arbeit mit OpenAPI. Dieser Port wird auch zur Annahme von Verbindungen von der Kaspersky Security Center Web Console verwendet. Optionale Angabe. der Standardwert ist 13299.	Portnummer
`KLSRV_UNATT_PORT_GUI`	Nein	Die Portnummer für die Arbeit mit klakaut-Tool. Optional. Standardwert ist 13291. Das Tool "klakaut" und das entsprechende Hilfesystem befinden sich im Installationsordner von Kaspersky Security Center Linux. Dieser Port ist standardmäßig geschlossen. Wenn Sie das Tool "klakaut" verwenden möchten, um die Vorgänge von Kaspersky Security Center Linux zu automatisieren, öffnen Sie den Port 13291 anhand des Tools "klscflag".	Portnummer
`KLSRV_UNATT_NETRANGETYPE`	Nein	Die ungefähre Anzahl an Geräten, die Sie verwalten möchten: Diese Einstellung wird zur Optimierung der Netzwerkauslastung verwendet. Optional. Standardwert ist 1.	`1` für 1 bis 100 verwaltete Geräte. `2` für 101 bis 1.000 verwaltete Geräte. `3` für mehr als 1.000 verwaltete Geräte.

`KLSRV_UNATT_DBMS_TYPE`	Ja	Der Typ des Datenbankverwaltungssystems: MySQL (MariaDB) oder Postgres.	`mysql`
			oder
			`postgres`

KLSRV_UNATT_DBMS_INSTANCE	Ja	Die IP-Adresse des Datenbankservers. Um PostgreSQL, ein Built-in High Availability-Cluster (BiHa) von Postgres Pro oder ein DBMS-Cluster von Platform V Pangolin zu verwenden, geben Sie für alle Knoten die DNS-Namen oder die IP-Adressen mit Ports im folgenden Format an: `<fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>;` Wenn Sie ein DBMS-Cluster von Platform V Pangolin verwenden, können Sie alternativ beim Angeben der DBMS-Adresse nur den DNS-Namen oder die IP-Adresse des primären Knotens oder Replika-Knotens angeben.	IP-Adresse
KLSRV_UNATT_DBMS_PORT	Ja	Der Port des Datenbankservers. Der Standardwert für MySQL (MariaDB) ist 3306. Der Standardwert für Postgres ist 5432.	`3306` oder `5432`
KLSRV_UNATT_DB_NAME	Ja	Der Name der Datenbank. Der Name der Datenbank muss sich von dem Namen der IAM-Datenbank, der in der Variablen `KLSRV_UNATT_DB_IAM_NAME` angegeben ist, unterscheiden.	`kav`
KLSRV_UNATT_DBMS_LOGIN	Ja	Der Benutzername eines Benutzers, der Zugriff auf die Datenbank hat.	
KLSRV_UNATT_DBMS_PASSWORD	Ja	Das Kennwort eines Benutzers, der Zugriff auf die Datenbank hat.	
KLSRV_UNATT_DBMS_SCHEMA	Nein	Das benutzerdefinierte DBMS-Schema. Wenn Sie kein benutzerdefiniertes Schema angeben, verwendet der Administrationsserver ein Standardschema. Beim Namen des Schemas muss die Groß- und Kleinschreibung beachtet werden: Sie dürfen nur Kleinbuchstaben verwenden. Ein benutzerdefiniertes Schema kann nur dann angegeben werden, wenn PostgreSQL oder Postgres Pro als DBMS verwendet wird. Andernfalls wird die Variable ignoriert.	`database_schema`
KLSRV_UNATT_IAM_ADDRESS	Nein	Die Browser der Benutzer werden von OpenIDConnect an diese Adresse umgeleitet. Geben Sie den FQDN des IAM-Servers ein. Sie müssen den DNS-Namen des Administrationsservers verwenden, der im Parameter `KLSRV_UNATT_SERVERADDRESS` angegeben wurde.	FQDN
KLSRV_UNATT_KLIAMUSER	Ja	Der Name des Benutzerkontos zum Starten des IAM-Dienstes. Das Benutzerkonto muss Mitglied der Sicherheitsgruppe sein, die in der Variablen `KLSRV_UNATT_KLADMINSGROUP` angegeben ist.	ksciam

KLSRV_UNATT_DBMS_IAM_TYPE	Ja	Der Typ des IAM-DBMS: MySQL (MariaDB) oder Postgres.	`mysql`
			oder
			`postgres`

KLSRV_UNATT_DBMS_IAM_INSTANCE	Ja	Die Adresse des IAM-Datenbankservers. Um PostgreSQL, ein Built-in High Availability-Cluster (BiHa) von Postgres Pro oder ein DBMS-Cluster von Platform V Pangolin zu verwenden, geben Sie für alle Knoten die DNS-Namen oder die IP-Adressen mit Ports im folgenden Format an: `<fqdn1>:<port>,<fqdn2>:<port>,<...> <fqdnX>:<port>;` Wenn Sie ein DBMS-Cluster von Platform V Pangolin verwenden, können Sie alternativ beim Angeben der DBMS-Adresse nur den DNS-Namen oder die IP-Adresse des primären Knotens oder Replika-Knotens angeben.	IP-Adresse
KLSRV_UNATT_DBMS_IAM_PORT	Ja	Der Port des IAM-Datenbankservers. Der Standardwert für MySQL (MariaDB) ist 3306. Der Standardwert für Postgres ist 5432.	3306 oder 5432
KLSRV_UNATT_DBMS_IAM_LOGIN	Ja	Der Benutzername eines Benutzers mit Zugriff zur IAM-Datenbank. Wenn es sich bei der IAM-Datenbank um MySQL (MariaDB) handelt und sie beide der folgenden Einstellungen aufweist: • `gtid_mode=ON` • `gtid_purged=ON|AUTO` Stellen Sie sicher, dass der angegebene Benutzer über eine der folgenden DBMS-Berechtigungen verfügt: • `RELOAD` • `FLUSH_TABLES`	
KLSRV_UNATT_DBMS_IAM_PASSWORD	Ja	Das Kennwort eines Benutzers mit Zugriff zur IAM-Datenbank.	
KLSRV_UNATT_DBMS_IAM_SCHEMA	Nein	Das benutzerdefinierte DBMS-Schema. Wenn Sie kein benutzerdefiniertes Schema angeben, verwendet IAM ein "public"-Schema. Ein benutzerdefiniertes Schema kann nur dann angegeben werden, wenn PostgreSQL oder Postgres Pro als DBMS verwendet wird. Andernfalls wird die Variable ignoriert. Beim Namen des Schemas wird die Groß- und Kleinschreibung berücksichtigt: Sie dürfen nur Kleinbuchstaben verwenden. Die folgenden Namen sind bereits von IAM reserviert und dürfen ebenfalls nicht angegeben werden: `client, iam, ksc, locker, pat, scope, voltron`.	`database_schema`
KLSRV_UNATT_DB_IAM_NAME	Ja	Der Name der IAM-Datenbank. Der Name der IAM-Datenbank muss sich von dem Namen der Datenbank, der in der Variablen `KLSRV_UNATT_DB_NAME` angegeben ist, unterscheiden. Geben Sie eine leere, manuell erstellte Datenbank an.	`iamdb`
KLSRV_UNATT_KLADMINSGROUP	Ja	Der Name der Sicherheitsgruppe für die Dienste.	`kladmins`

KLSRV_UNATT_KLSRVUSER	Ja	Der Name des Benutzerkontos zum Starten des Administrationsserver-Dienstes. Das Benutzerkonto muss Mitglied der Sicherheitsgruppe sein, die in der Variablen KLSRV_UNATT_KLADMINSGROUP angegeben ist.	ksc
KLSRV_UNATT_KLSVCUSER	Ja	Der Name des Benutzerkontos zum Starten anderer Dienste. Das Benutzerkonto muss Mitglied der Sicherheitsgruppe sein, die in der Variablen KLSRV_UNATT_KLADMINSGROUP angegeben ist.	ksc
Für eine Bereitstellung eines Administrationsservers, der als Kaspersky Security Center Linux Failover-Cluster fungiert, muss die Antwortdatei die folgenden zusätzlichen Variablen enthalten:			
KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT	Nein	Die Konfiguration des Failover-Clusters. Wenn der Parameter in der Antwortdatei fehlt, wird der Standardwert verwendet. Mögliche Werte: 0 – Failover-Cluster, dessen Knoten sich in einem einzelnen Rechenzentrum befinden (Standardwert). 2 – Geografisch verteiltes Failover-Cluster, dessen Knoten sich in verschiedenen Rechenzentren befinden.	0 oder 2
KLFOC_UNATT_NODE	Ja	Die Nummer des Knotens (1 oder 2).	1 oder 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Ja	Der State Share-Einhängepunkt.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Ja	Der Data Share-Einhängepunkt.	
KLFOC_UNATT_CONN_MODE	Ja	Der Konnektivitätsmodus des Failover-Clusters.	VirtualAdapter oder ExternalLoadBalancer
Falls die Variable KLFOC_UNATT_CONN_MODE den Wert VirtualAdapter besitzt, muss die Antwortdatei die folgenden zusätzlichen Variablen enthalten:			
KLFOC_UNATT_CONN_MODE_VA_NAME	Ja	Der Name des virtuellen Netzwerkadapters.	
KLFOC_UNATT_CONN_MODE_VA_IPV4	Eine dieser Variablen ist erforderlich	Die IP-Adresse des virtuellen Netzwerkadapters.	IP-Adresse
KLFOC_UNATT_CONN_MODE_VA_IPV6		Die IPv6-Adresse des virtuellen Netzwerkadapters.	IPv6-Adresse

Kaspersky Security Center Linux unter Astra Linux in der geschlossenen Softwareumgebung installieren

Dieser Abschnitt beschreibt die Installation von Kaspersky Security Center Linux auf dem Betriebssystem Astra Linux Special Edition.

Vor der Installation:

- Installieren Sie das DBMS.
- Laden Sie den Anwendungsschlüssel kaspersky_astra_pub_key.gpg herunter.
- Laden Sie die Installationsdatei ksc64_[Versionsnummer]_amd64.deb von der Kaspersky-Website herunter.

Führen Sie die Befehle in dieser Anleitung unter einem Benutzerkonto mit Root-Berechtigung und mit hoher Integrität und ohne Vertraulichkeit aus.

So installieren Kaspersky Security Center Linux auf den Betriebssystemen Astra Linux Special Edition (operatives Update 1.7.2) und Astra Linux Special Edition (operatives Update 1.6):

1. Öffnen Sie die Datei `/etc/digsig/digsig_initramfs.conf` und geben Sie die folgende Einstellung an:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Führen Sie in der Befehlszeile den folgenden Befehl aus, um das Kompatibilitätspaket zu installieren:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Erstellen Sie ein Verzeichnis für den Anwendungsschlüssel:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Legen Sie den Anwendungsschlüssel in das Verzeichnis ab, das im vorherigen Schritt erstellt wurde:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

5. Aktualisieren Sie das ursprüngliche RAM-Image des Dateisystems für alle Kernel des Systems:

   ```
   update-initramfs -u -k all
   ```

   Starten Sie das System neu.

6. Erstellen Sie die Gruppe "kladmins" und die nicht-privilegierten Konten "ksc" und "ksciam". Das Benutzerkonto muss Mitglied der Gruppe "kladmins" sein. Führen Sie dazu nacheinander die folgenden Befehle aus:

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   # adduser ksciam
   # gpasswd -a ksciam kladmins
   # usermod -g kladmins ksciam
   ```

7. Starten Sie die Installation von Kaspersky Security Center Linux:

   ```
   # apt install /<path>/ksc64_[ Versionsnummer ]_amd64.deb
   ```

8. Führen Sie die Konfiguration von Kaspersky Security Center Linux aus:

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

9. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA) und die Datenschutzrichtlinie. Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie bei Aufforderung die folgenden Werte ein:

    a. Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren. Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der EULA zustimmen.

    b. Geben Sie `y` ein, wenn Sie die Bedingungen der Datenschutzrichtlinie verstehen und akzeptieren, und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Geben Sie `n` ein, wenn Sie den Bedingungen der Datenschutzrichtlinie nicht zustimmen. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der Datenschutzrichtlinie zustimmen.

10. Geben Sie nach der entsprechenden Aufforderung die folgenden Einstellungen ein:

    a. Geben Sie den DNS-Namen oder die statische IP-Adresse des Administrationsservers ein.

    b. Geben Sie die Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 14000 festgelegt.

    c. Geben Sie die SSL-Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 13000 festgelegt.

    d. Ermitteln Sie die ungefähre Anzahl der Geräte, die Sie verwalten möchten:

    - Geben Sie für 1 bis 100 verwaltete Geräte den Wert 1 ein.
    - Geben Sie für 101 bis 1.000 verwaltete Geräte den Wert 2 ein.
    - Geben Sie für über 1.000 verwaltete Geräte den Wert 3 ein.

    Diese Einstellung dient der automatischen, zufälligen Verzögerung von Aufgabenstarts, um die Auslastung auf das Netzwerk zu optimieren. Die folgende Liste enthält die Intervalle, innerhalb denen die Verzögerung berechnet wird:

    - 1 bis 100 verwaltete Geräte, Wert 1. Es wird keine Verzögerung verwendet.
    - 101 bis 1.000 verwaltete Geräte, Wert 2. Die Verzögerung beträgt 5 Minuten.
    - Über 1.000 verwaltete Geräte, Wert 3. Die Verzögerung beträgt 10 Minuten.

    e. Geben Sie den Namen der Sicherheitsgruppe für Dienste ein. Standardmäßig wird die Gruppe 'kladmins' verwendet.

    f. Geben Sie den Namen des Benutzerkontos ein, um den Administrationsserver-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto 'ksc' verwendet.

    g. Geben Sie den Namen des Benutzerkontos ein, um andere Dienste zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto 'ksc' verwendet.

    h. Wählen Sie das DBMS aus, das Sie für die Verwendung mit Kaspersky Security Center Linux installiert haben:

    - Wenn Sie MySQL oder MariaDB installiert haben, geben Sie "1" ein.
    - Wenn Sie PostgreSQL oder Postgres Pro installiert haben, geben Sie "2" ein.

i. Geben Sie die IP-Adresse des Gerätes ein, auf dem die Datenbank installiert ist.

j. Geben Sie die Portnummer der Datenbank ein. Dieser Port wird für die Kommunikation mit dem Administrationsserver verwendet. Standardmäßig werden die folgenden Ports verwendet:

- Port 3306 für MySQL oder MariaDB.
- Port 5432 für PostgreSQL oder Postgres Pro.

k. Geben Sie den Namen der Datenbank ein.

l. Geben Sie den Benutzernamen für das Konto des Datenbank-Administrators ein, das Sie für den Zugriff auf die Datenbank verwenden.

m. Geben Sie das Kennwort für das Konto des Datenbank-Administrators ein, das Sie für den Zugriff auf die Datenbank verwenden.

n. Geben Sie den FQDN-Namen des IAM-Servers ein.

Sie müssen den DNS-Namen des Administrationsservers angeben, den Sie in Schritt 10a eingegeben haben.

o. Geben Sie den Namen des Benutzerkontos ein, um den kliam-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein.

p. Wählen Sie das DBMS aus, das Sie für die Verwendung des IAM-Dienstes installiert haben:

- Wenn Sie MySQL oder MariaDB installiert haben, geben Sie "1" ein.
- Wenn Sie PostgreSQL oder Postgres Pro installiert haben, geben Sie "2" ein.

q. Geben Sie die DBMS-Adresse ein, die der IAM-Dienst verwenden soll.

r. Geben Sie die Portnummer der Datenbank ein. Dieser Port wird für die Kommunikation mit dem IAM-Dienst verwendet. Standardmäßig werden die folgenden Ports verwendet:

- Port 3306 für MySQL oder MariaDB.
- Port 5432 für PostgreSQL oder Postgres Pro.

s. Geben Sie den Namen der Datenbank ein, den der IAM-Dienst verwenden soll. Der Name der vom IAM-Dienst verwendeten Datenbank muss sich von der Datenbank unterscheiden, die vom Administrationsserver verwendet wird.

t. Geben Sie den Benutzernamen des Datenbank-Root-Kontos ein, das Sie für den Zugriff auf die IAM-Datenbank verwenden.

u. Geben Sie das Kennwort des Datenbank-Root-Kontos ein, das Sie für den Zugriff auf die IAM-Datenbank verwenden.

Warten Sie, bis die Dienste hinzugefügt und automatisch gestartet wurden:

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`

- `klwebsrv_srv`
- `kliam_srv`

v. Erstellen Sie ein Benutzerkonto, das als Administrator des Administrationsservers fungiert. Geben Sie den Benutzernamen und das Kennwort ein.

Das Kennwort muss den folgenden Regeln entsprechen:

- Das Benutzerkennwort muss aus mindestens 8 und maximal 256 Zeichen bestehen.
- Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
  - Großbuchstaben (A–Z)
  - Kleinbuchstaben (a–z)
  - Ziffern (0–9)
  - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Kaspersky Security Center Linux wird installiert und der Benutzer wird hinzugefügt.

Überprüfung von Diensten

Verwenden Sie die folgenden Befehle, um zu überprüfen, ob ein Dienst ausgeführt wird oder nicht:

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`
- `# systemctl status kliam_srv.service`

Kaspersky Security Center Web Console installieren

In diesem Abschnitt wird beschrieben, wie Sie den Server der Web Console von Kaspersky Security Center (auch als Kaspersky Security Center Web Console bezeichnet) auf Geräten mit Linux-Betriebssystemen installieren. Vor der Installation müssen Sie ein DBMS und den Kaspersky Security Center Linux Administrationsserver installieren.

Wenn Sie Kaspersky Security Center Web Console unter Astra Linux in der abgeschlossenen Softwareumgebung installieren, befolgen Sie die spezifischen Anweisungen für Astra Linux.

Verwenden Sie eine der folgenden Installationsdateien, je nach der Linux-Distribution, die auf Ihrem Gerät installiert ist:

- Für Debian: ksc-web-console-<Build-Nummer>.x86_64.deb
- Für RPM-basierte Betriebssysteme: ksc-web-console-<Build-Nummer>.x86_64.rpm

Sie erhalten die Installationsdatei, indem Sie diese von der Kaspersky-Website herunterladen.

So installieren Sie Kaspersky Security Center Web Console:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center Web Console installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.
2. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA). Wenn das Programmpaket von Kaspersky Security Center Linux keine txt-Datei mit dem Text der EULA enthält, können Sie die Datei von der Kaspersky-Website herunterladen. Falls Sie den Lizenzvertrag ablehnen, installieren Sie die Anwendung nicht.
3. Erstellen Sie eine Antwortdatei mit Parametern für die Verbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver: `/etc/ksc-web-console-setup.json`.

   Beispiel für eine Antwortdatei mit den minimal notwendigen Parametern

   Die Gruppe an Parametern in der Antwortdatei hängt von der Version des Administrationsservers ab, mit welcher die Kaspersky Security Center Web Console verbunden ist:

   - Administrationsserver ab Version 16

     Beispiel für eine Antwortdatei mit minimalen Parametern für die Anmeldung am Administrationsserver Version 16 oder höher:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Administrationsserver Version 15.4 oder niedriger

  Beispiel für eine Antwortdatei mit minimalen Parametern für die Anmeldung am Administrationsserver Version 15.4 oder niedriger:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Sie können die Kaspersky Security Center Web Console entweder auf demselben Gerät, auf dem der Administrationsserver installiert ist, oder auf einem anderen Gerät installieren. Wenn die Kaspersky Security Center Web Console auf einem anderen Gerät installiert ist, unterscheidet sich die Adresse der Kaspersky Security Center Web Console (durch `address` angegeben) von der Adresse des Administrationsservers (durch `iamHost` oder `kscHost` angegeben). Wenn die Kaspersky Security Center Web Console und der Administrationsserver auf demselben Gerät installiert sind, besitzen diese Parameter die gleichen Werte.

Der Wert `iamHost` muss mit der IAM-Adresse übereinstimmen, die Sie bei der Installation des Administrationsservers angegeben haben. Um die angegebene IAM-Adresse zu erhalten, führen Sie folgenden Befehl auf dem Gerät mit dem installierten Administrationsserver aus:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Weiter Informationen dazu finden Sie in folgendem Artikel: Installationsparameter für Kaspersky Security Center Web Console.

Sie können der Liste der vertrauenswürdigen Server mehrere Administrationsserver unterschiedlicher Versionen hinzufügen. In diesem Fall können die Server unterschiedliche Authentifizierungsmethoden verwenden.

Es wird empfohlen, Portnummern oberhalb von 1024 anzugeben. Wenn Sie möchten, dass Kaspersky Security Center Web Console auf den Ports unterhalb von 1024 funktioniert, stellen Sie nach der Installation sicher, dass Sie über das Tool "setcap" verfügen, und führen Sie den folgenden Befehl aus:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

Wenn Sie das setcap-Tool nicht besitzen, können Sie es installieren. **Klicken Sie auf diesen Link, um die Befehle anzuzeigen**.

Führen Sie für die Debian- und Ubuntu-Betriebssysteme einen der folgenden Befehle aus:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Führen Sie für SUSE Linux Enterprise Server und Red Hat Enterprise Linux den folgenden Befehl aus:

- `sudo zypper install libcap-progs`

Wenn Sie die Kaspersky Security Center Web Console auf dem Betriebssystem ALT Linux installieren, müssen Sie eine andere Portnummer als 8080 angeben, da Port 8080 vom Betriebssystem verwendet wird.

Kaspersky Security Center Web Console kann nicht aktualisiert werden, wenn dafür die gleiche rpm-Installationsdatei verwendet wird. Wenn Sie die Einstellungen in einer Antwortdatei ändern und diese Datei zur Neuinstallation der Anwendung verwenden möchten, müssen Sie die Anwendung zunächst löschen und sie anschließend mit der neuen Antwortdatei erneut installieren.

4. Führen Sie unter einem Konto mit Root-Berechtigungen mithilfe der Befehlszeile und abhängig von Ihrer Linux-Distribution die Setup-Datei mit der Erweiterung .deb oder .rpm aus.

   - Um Kaspersky Security Center Web Console aus einer .deb-Datei zu installieren oder zu aktualisieren, führen Sie den folgenden Befehl aus:
     ```
     sudo apt-get install ksc-web-console-<Build-Nummer>.x86_64.deb
     ```
   - Um Kaspersky Security Center Web Console aus einer .rpm -Datei zu installieren, führen Sie einen der folgenden Befehl aus:
     ```
     sudo yum install ksc-web-console-<Build-Nummer>.x86_64.rpm
     ```
     oder
     ```
     sudo alien -i ksc-web-console-<Build-Nummer>.x86_64.rpm
     ```
   - Um von einer früheren Version von Kaspersky Security Center Web Console zu aktualisieren, führen Sie einen der folgenden Befehle aus:
     - Für Geräte mit RPM-basiertem Betriebssystem:
       ```
       sudo yum install ksc-web-console-<Build-Nummer>.x86_64.rpm
       ```
     - Für Geräte mit Debian-basiertem Betriebssystem:
       ```
       sudo apt-get install ksc-web-console-<Build-Nummer>.x86_64.deb
       ```

   Dadurch wird die Installationsdatei entpackt. Bitte warten Sie, bis die Installation abgeschlossen ist. Kaspersky Security Center Web Console wird in den folgenden Pfad installiert: /var/opt/kaspersky/ksc-web-console.

5. Starten Sie alle Dienste von Kaspersky Security Center Web Console neu, indem Sie den folgenden Befehl ausführen:
   ```
   sudo systemctl restart KSC*
   ```

Nach dem erfolgreichen Abschluss der Installation können Sie in Ihrem Browser Kaspersky Security Center Web Console öffnen und sich einloggen.

Wenn das allgemeine Zertifikat des Administrationsservers durch ein anderes Zertifikat aus einer Sicherung oder mithilfe des Tools "klsetsrvcert" ersetzt wird, müssen Sie die Kaspersky Security Center Web Console entfernen und anschließend neu installieren. Andernfalls wird der Zugriff auf die Web Console eingeschränkt. Wenn Sie sich nach der Neuinstallation nicht an der Web Console anmelden können, überprüfen Sie die Konfiguration des IAM-Servers.

Installationsparameter für Kaspersky Security Center Web Console

Für die Installation des Servers der Web Console von Kaspersky Security Center auf Linux-Geräten, müssen Sie eine Antwortdatei erstellen. Dies muss eine .json-Datei sein, welche die Parameter für die Verbindung von Kaspersky Security Center Web Console mit dem Administrationsserver enthält. Sie müssen diese Datei "ksc-web-console-setup.json" nennen und in das Verzeichnis "/etc/ksc-web-console-setup.json" legen.

Die Gruppe an Parametern in der Antwortdatei hängt von der Version des Administrationsservers ab, mit welcher die Kaspersky Security Center Web Console verbunden ist.

- Administrationsserver ab Version 16

  Der Administrationsserver in Version 16 oder höher bietet die Identitäts- und Zugriffsverwaltung (IAM), welche die Domänenauthentifizierung mit Single Sign-On (SSO) in der Kaspersky Security Center Web Console bereitstellt. Damit sich die Kaspersky Security Center Web Console mit dem Administrationsserver verbinden kann, muss die Antwortdatei die Parameter zur Interaktion mit der IAM-Komponente selbst dann enthalten, wenn Sie das einmalige Anmelden (SSO) nicht verwenden.

  Beispiel für eine Antwortdatei für die Installation einer Web Console, die eine Verbindung zum Administrationsserver Version 16 oder höher herstellt. In diesem Beispiel sind die Web Console und der Administrationsserver auf unterschiedlichen Geräten installiert:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v16": {
    "iamHost": "ksc16.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
    "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "messageQueueAccount": "Group1:User5",
    "natsMessageQueueAccount": "Group1:User6"
}
```

- Administrationsserver Version 15.4 oder niedriger

  Der Administrationsserver 15.4 oder niedriger unterstützt die Authentifizierung nur durch Angabe von Name und Kennwort des internen Benutzers oder des Domänenbenutzers.

  Beispiel für eine Antwortdatei für die Installation einer Web Console, die eine Verbindung zum Administrationsserver Version 15.4 oder niedriger herstellt:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "defaultLangId": 1049,
    "enableLog": true,
    "trusted":  {
        "Administration Server v15.4": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
```

```
    "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "acceptEula": true,
    "certPath": "/root/server.crt",
    "keyPath": "/root/key-without-passphrase.pem",
    "webConsoleAccount": "Group1:User1",
    "managementServiceAccount": "Group1:User2",
    "serviceWebConsoleAccount": "Group1:User3",
    "pluginAccount": "Group1:User4",
    "messageQueueAccount": "Group1:User5",
    "natsMessageQueueAccount": "Group1:User6"
}
```

Die Parameter`webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, `messageQueueAccount`, `natsMessageQueueAccount`, `certPath` und `keyPath` sind optional. Sie können diese Parameter in der Antwortdatei weglassen.

Wenn Sie ein benutzerdefiniertes Zertifikat verwenden möchten, geben Sie die Parameter `certPath` und `keyPath` an. Wenn Sie keine oder nur einen Parameter angeben, informiert Sie der Webbrowser weiterhin darüber, dass Ihre Verbindung nicht privat ist.

Aus Sicherheitsgründen wird davon abgeraten, die Parameter `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, `messageQueueAccount` und `natsMessageQueueAccount` anzugeben.
Wenn Sie sich für die Angabe dieser Parameter entscheiden, stellen Sie sicher, dass die benutzerdefinierten Benutzerkonten derselben Sicherheitsgruppe angehören. Wenn keine Parameter angegeben werden, erstellt der Installer der Kaspersky Security Center Web Console zunächst eine Standard-Sicherheitsgruppe und anschließend Benutzerkonten mit Standardnamen innerhalb dieser Gruppe.
Die Parameter `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, `messageQueueAccount` und `natsMessageQueueAccount` dürfen nicht getrennt voneinander verwendet werden: Geben Sie die Werte entweder für alle diese Parameter oder für keinen von ihnen an.

Sie können die Kaspersky Security Center Web Console entweder auf demselben Gerät, auf dem der Administrationsserver installiert ist, oder auf einem anderen Gerät installieren. Wenn die Kaspersky Security Center Web Console auf einem anderen Gerät installiert ist, unterscheidet sich die Adresse der Kaspersky Security Center Web Console (durch `address` angegeben) von der Adresse des Administrationsservers (durch `iamHost` oder `kscHost` angegeben). Wenn die Kaspersky Security Center Web Console und der Administrationsserver auf demselben Gerät installiert sind, besitzen diese Parameter die gleichen Werte.

Der Wert `iamHost` muss mit der IAM-Adresse übereinstimmen, die bei der Installation des Administrationsservers angegeben wurde. Um die angegebene IAM-Adresse zu erhalten, führen Sie folgenden Befehl auf dem Host des Administrationsservers aus:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Es wird empfohlen, Portnummern oberhalb von 1024 anzugeben. Wenn Sie möchten, dass die Kaspersky Security Center Web Console auf Ports unterhalb von 1024 funktioniert, müssen Sie nach der Installation den folgenden Befehl ausführen:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

Wenn Sie das setcap-Tool nicht besitzen, können Sie es installieren. **Klicken Sie auf diesen Link, um die Befehle anzuzeigen**.

Führen Sie für die Debian- und Ubuntu-Betriebssysteme einen der folgenden Befehle aus:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Führen Sie für SUSE Linux Enterprise Server und Red Hat Enterprise Linux den folgenden Befehl aus:

- `sudo zypper install libcap-progs`

Wenn Sie die Kaspersky Security Center Web Console auf dem ALT Linux-Betriebssystem installieren, müssen Sie eine andere Portnummer als 8080 angeben, da Port 8080 von dem Betriebssystem verwendet wird.

In der folgenden Tabelle werden die Parameter beschrieben, die in einer Antwortdatei angegeben werden können.

Parameter für die Installation von Kaspersky Security Center Web Console auf Geräten mit Linux

Parameter	Beschreibung	Mögliche Werte
`address`	Adresse des Geräts (FQDN oder Hostname) mit installierter Kaspersky Security Center Web Console (erforderlich). Wenn Sie die Kaspersky Security Center Web Console auf dem Server von Kaspersky Security Center installieren, verwenden Sie die Adresse, die Sie bei der Installation von Kaspersky Security Center Linux angegeben haben. Wenn Sie die Kaspersky Security Center Web Console auf einem anderen Gerät installieren, geben Sie die Adresse (FQDN oder Hostname) des Geräts an, die der Webbrowser für die Verbindung mit dem Server der Kaspersky Security Center Web Console verwenden soll.	Zeichenfolgenwert. Beispiel: `"ksc.example.com"`
`port`	Port, der von Kaspersky Security Center Web Console verwendet wird, um Verbindungen von Webbrowsern zu empfangen (erforderlich).	Zahlenwert. Der empfohlene Wert ist 8080 (mit Ausna Betriebssystem ALT Linux-Betriebssyste
`defaultLangId`	Sprache der Benutzeroberfläche (standardmäßig `1033`). Falls erforderlich können Sie die Sprache der Benutzeroberfläche von Kaspersky Security Center Web Console ändern.	Zahlencodes der Sprachen: • Deutsch: `1031` • Englisch: `1033` • Spanisch: `1034` • Spanisch (Mexiko): `2058` • Französisch: `1036` • Italienisch: `1040` • Japanisch: `1041` • Kasachisch: `1087` • Polnisch: `1045` • Portugiesisch (Brasilien): `1046` • Russisch: `1049` • Türkisch: `1055` • Vereinfachtes Chinesisch: `2052` • Traditionelles Chinesisch: `1028` Wenn kein Wert angegeben ist, wird Engli verwendet.
`enableLog`	Gibt an, ob die Aktivitätsprotokollierung in Kaspersky Security Center Web Console aktiviert werden soll oder nicht. Wie empfehlen, den Standardwert für den Parameter nur auf Anfrage eines technischen Kaspersky Support-Mitarbeiters zu ändern.	Boolescher Wert: • `true` – Protokollierung aktiviert. • `false` – Protokollierung deaktiviert (ausgewählt).

Parameter	Beschreibung	Mögliche Werte
`trusted`	Liste mit Adressen vertrauenswürdiger Administrationsserver, mit denen sich Kaspersky Security Center Web Console verbinden kann. Sie können der Liste der vertrauenswürdigen Server mehrere Administrationsserver unterschiedlicher Versionen hinzufügen. Für Administrationsserver ab Version 16: • Der im Login-Fenster anzuzeigende Name des Administrationsservers. • `iamHost` entspricht der Adresse (FQDN oder Hostname) des Administrationsservers, der die IAM-Komponente enthält (beginnend mit Kaspersky Security Center Linux Version 16) und mit dem sich Kaspersky Security Center Web Console verbindet. Der Wert `iamHost` muss mit der IAM-Adresse übereinstimmen, die bei der Installation des Administrationsservers angegeben wurde. Um die angegebene IAM-Adresse zu erhalten, führen Sie folgenden Befehl auf dem Host des Administrationsservers aus: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` • `iamOAuthPort` dem Port entspricht, der für den Austausch der Authentifizierungstoken über das OpenID Connect-Authentifizierungsprotokoll verwendet wird (der Standardwert beträgt 4444). Dieser Port wird sowohl für die Kommunikation zwischen dem Server der Kaspersky Security Center Web Console und dem Administrationsserver als auch zwischen dem Browser (in dem Kaspersky Security Center Web Console verwendet wird) und dem Administrationsserver verwendet. • `iamProxyPort` entspricht dem Port, der zur Verbindung des Servers der Kaspersky Security Center Web Console mit dem Administrationsserver verwendet wird (der Standardwert beträgt 9050). • `iamCertPath` entspricht dem Pfad zum IAM-Zertifikat. Das IAM-Zertifikat wird beim ersten Start des Administrationsservers automatisch erstellt. Die Zertifikatsdatei befindet sich auf dem Gerät, auf dem der Administrationsserver installiert ist. Der Standardpfad des Zertifikats lautet: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem. Das selbstsignierte IAM-Zertifikat wird automatisch rotiert. • `iamPATPath` entspricht dem Pfad des Tokens, der für die Registrierung der Kaspersky Security Center Web Console als OAuth-Client in der IAM verwendet wird. Die Datei wird beim ersten Start des Administrationsservers automatisch erstellt. Das Token befindet sich auf dem Gerät mit dem installierten Administrationsserver. Der Standardpfad des Tokens lautet: /var/opt/kaspersky/klnagent_srv/iam/initial_token.txt. Das Token ist unbegrenzt gültig und erfordert keine Rotation. • `kscPort` entspricht dem Port, der für die Verbindung der Kaspersky Security Center Web Console zum Administrationsserver über OpenAPI verwendet wird (der Standardwert beträgt 13299). • `kscCertPath` entspricht dem Pfad zum Zertifikat des Administrationsservers. Die Zertifikatsdatei befindet sich auf dem Gerät, auf dem der Administrationsserver installiert ist. Der Standardpfad zum Zertifikat lautet: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer.	Ein Abschnitt aus der JSON-Datei im folg `"trusted": { "Administration Server v16": { "iamHost": "ksc-iam.example.com", "iamOAuthPort": 4444, "iamProxyPort": 9050, "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_c "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initia "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ }, "Administration Server v15.4": { "kscHost": "ksc.example.com", "kscPort": 13299, "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/ } }`  Anstelle von `Administration Server Administration Server v15.4` könne Namen für die Administrationsserver ang

Parameter	Beschreibung	Mögliche Werte
	Für Administrationsserver der Version 15.4 oder niedriger: • Der im Login-Fenster anzuzeigende Name des Administrationsservers. • `kscHost` entspricht der Adresse (FQDN oder Hostname) des Administrationsservers, mit dem sich Kaspersky Security Center Web Console verbindet. • `kscPort` entspricht dem OpenAPI-Port, der zur Verbindung des Servers der Kaspersky Security Center Web Console mit dem Administrationsserver verwendet wird (der Standardwert beträgt 13299). • `kscCertPath` entspricht dem Pfad zum Zertifikat des Administrationsservers. Die Zertifikatsdatei befindet sich auf dem Gerät, auf dem der Administrationsserver installiert ist. Der Standardpfad zum Zertifikat lautet: /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer. Bei der Installation der Kaspersky Security Center Web Console auf einem externen Gerät, dass kein Administrationsserver ist, kopieren Sie die Dateien des Administrationsserver-Zertifikats (angegeben durch `kscCertPath`), des IAM-Zertifikats (angegeben durch `iamCertPath`) und des Token (angegeben durch `iamPATPath`) vom Gerät mit dem installiertem Administrationsserver auf das Zielgerät. Geben Sie den lokalen Pfad zu diesen Dateien in der Antwortdatei für das Installationsprogramm von Web Console an.	
`acceptEula`	Gibt an, ob Sie die Bedingungen des Endbenutzer-Lizenzvertrags (EULA) akzeptieren oder nicht. Die Datei mit den Bedingungen der EULA wird zusammen mit der Installationsdatei heruntergeladen.	Boolescher Wert: • `true` – Ich bestätige, dass ich die Be und Bedingungen dieses Endbenutze Lizenzvertrags vollständig gelesen ha verstehe und akzeptiere. • `false` – Ich akzeptiere die Bedingun Endbenutzer-Lizenzvertrags nicht (s ausgewählt). Wenn kein Wert angegeben ist, zeigt Ihne Installationsprogramm der Kaspersky Sec Web Console die EULA an und fragt nach Bedingungen der EULA zustimmen oder n
`certDomain`	Wenn Sie ein neues selbstsigniertes Zertifikat erstellen möchten, geben Sie mithilfe dieses Parameters den FQDN für die Verbindung des Webbrowsers mit der Kaspersky Security Center Web Console an.	Zeichenfolgenwert.
`certPath`	Verwenden Sie den Parameter, um den Pfad des benutzerdefinierten Zertifikats für Kaspersky Security Center Web Console anzugeben, das in Ihrer Infrastruktur vertrauenswürdig ist und die Anforderungen für benutzerdefinierte Zertifikate erfüllt. Sie können nur einen privaten Schlüssel (`keyPath`) für ein Zertifikat oder für eine Zertifikatskette angeben.	Zeichenfolgenwert. Verschlüsselte Zertifikate werden von Kas Security Center Web Console nicht unte Geben Sie auf dem Gerät, auf dem Kaspe Center Web Console installiert werden so der Zertifikatsdatei im PEM-Format an. Beispiel: `/root/server.crt`
`keyPath`	Verwenden Sie den Parameter, um den Pfad des privaten Schlüssels anzugeben, der mit dem benutzerdefinierten Zertifikat von Kaspersky Security Center Web Console verknüpft ist, das im Parameter `certPath` angegeben ist.	Zeichenfolgenwert. Die Datei mit dem privaten Schlüssel darf verschlüsselt sein. Geben Sie auf dem Gerät, auf dem Kaspe Center Web Console installiert werden so Schlüsseldatei im PEM-Format an. Beispiel: `/root/key-without-passphr`
`webConsoleAccount`	Name des Benutzerkontos, unter dem der Dienst Kaspersky Security Center Web Console ausgeführt wird.	Zeichenkette im folgenden Format: `"< Gr < Benutzername >"`. Beispiel: `"Group1:User1"`. Wenn kein Wert angegeben wird, erstellt Installationsprogramm von Kaspersky Sec Web Console ein neues Benutzerkonto m Standardnamen `user_management_%ui`

Parameter	Beschreibung	Mögliche Werte
`managementServiceAccount`	Name des Kontos, unter dem der Kaspersky Security Center Web Console Management Service ausgeführt wird.	Zeichenkette im folgenden Format: `"< Gr < Benutzername >"`. Beispiel: `"Group1:User2"`. Wenn kein Wert angegeben wird, erstellt Installationsprogramm von Kaspersky Sec Web Console ein neues Benutzerkonto m Standardnamen `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Name des Benutzerkontos, unter dem der Dienst Kaspersky Security Center Web Console ausgeführt wird.	Zeichenkette im folgenden Format: `"< Gr < Benutzername >"`. Beispiel: `"Group1:User3"`. Wenn kein Wert angegeben wird, erstellt Installationsprogramm von Kaspersky Sec Web Console ein neues Benutzerkonto m Standardnamen `user_svc_nodejs_%ui`
`pluginAccount`	Name des Benutzerkontos, unter dem der Dienst Kaspersky Security Center Product Plugins ausgeführt wird.	Zeichenkette im folgenden Format: `"< Gr < Benutzername >"`. Beispiel: `"Group1:User4"`. Wenn kein Wert angegeben wird, erstellt Installationsprogramm von Kaspersky Sec Web Console ein neues Benutzerkonto m Standardnamen `user_web_plugin_%ui`
`messageQueueAccount`	Name des Benutzerkontos, unter dem der Dienst Kaspersky Security Center Web Console Message Queue ausgeführt wird.	Zeichenkette im folgenden Format: `"< Gr < Benutzername >"`. Beispiel: `"Group1:User5".` Wenn kein Wert angegeben wird, erstellt Installationsprogramm von Kaspersky Sec Web Console ein neues Benutzerkonto m Standardnamen `user_message_queue_`
`natsMessageQueueAccount`	Name des Benutzerkontos, unter dem der Dienst Kaspersky Security Center Web Console NATS ausgeführt wird.	Zeichenkette im folgenden Format: `"< Gr < Benutzername >"`. Beispiel: `"Group1:User6"`. Wenn kein Wert angegeben wird, erstellt Installationsprogramm von Kaspersky Sec Web Console ein neues Benutzerkonto m Standardnamen `user_message_queue_`

Kaspersky Security Center Web Console unter Astra Linux in der geschlossenen Softwareumgebung installieren

In diesem Abschnitt wird beschrieben, wie Sie den Server der Web Console von Kaspersky Security Center (auch als Kaspersky Security Center Web Console bezeichnet) unter dem Betriebssystemen Astra Linux Special Edition installieren. Vor der Installation müssen Sie ein DBMS und den Kaspersky Security Center Linux Administrationsserver installieren.

So installieren Sie Kaspersky Security Center Web Console:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center Web Console installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

2. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA). Wenn das Programmpaket von Kaspersky Security Center Linux keine txt-Datei mit dem Text der EULA enthält, können Sie die Datei von der Kaspersky-Website herunterladen. Falls Sie den Lizenzvertrag ablehnen, installieren Sie die Anwendung nicht.

3. Erstellen Sie eine Antwortdatei mit Parametern für die Verbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver: `/etc/ksc-web-console-setup.json`.

   Beispiel für eine Antwortdatei mit den minimal notwendigen Parametern

Die Gruppe an Parametern in der Antwortdatei hängt von der Version des Administrationsservers ab, mit welcher die Kaspersky Security Center Web Console verbunden ist:

- Administrationsserver ab Version 16

  Beispiel für eine Antwortdatei mit minimalen Parametern für die Anmeldung am Administrationsserver Version 16 oder höher:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Administrationsserver Version 15.4 oder niedriger

  Beispiel für eine Antwortdatei mit minimalen Parametern für die Anmeldung am Administrationsserver Version 15.4 oder niedriger:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Sie können die Kaspersky Security Center Web Console entweder auf demselben Gerät, auf dem der Administrationsserver installiert ist, oder auf einem anderen Gerät installieren. Wenn die Kaspersky Security Center Web Console auf einem anderen Gerät installiert ist, unterscheidet sich die Adresse der Kaspersky Security Center Web Console (durch `address` angegeben) von der Adresse des Administrationsservers (durch `iamHost` oder `kscHost` angegeben). Wenn die Kaspersky Security Center Web Console und der Administrationsserver auf demselben Gerät installiert sind, besitzen diese Parameter die gleichen Werte.

Der Wert `iamHost` muss mit der IAM-Adresse übereinstimmen, die Sie bei der Installation des Administrationsservers angegeben haben. Um die angegebene IAM-Adresse zu erhalten, führen Sie folgenden Befehl auf dem Gerät mit dem installierten Administrationsserver aus:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Weiter Informationen dazu finden Sie in folgendem Artikel: Installationsparameter für Kaspersky Security Center Web Console.

Sie können der Liste der vertrauenswürdigen Server mehrere Administrationsserver unterschiedlicher Versionen hinzufügen. In diesem Fall können die Server unterschiedliche Authentifizierungsmethoden verwenden.

4. Öffnen Sie die Datei `/etc/digsig/digsig_initramfs.conf` und geben Sie die folgende Einstellung an:

```
DIGSIG_ELF_MODE=1
```

5. Führen Sie in der Befehlszeile den folgenden Befehl aus, um das Kompatibilitätspaket zu installieren:

```
apt install astra-digsig-oldkeys
```

6. Erstellen Sie ein Verzeichnis für den Anwendungsschlüssel:

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

7. Legen Sie den Anwendungsschlüssel `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` in dem Verzeichnis ab, das Sie beim vorherigen Schritt erstellt haben:

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

Wenn der Anwendungsschlüssel "kaspersky_astra_pub_key.gpg" nicht im Lieferumfang von Kaspersky Security Center Linux enthalten ist, können Sie den Schlüssel über den folgenden Link herunterladen: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Aktualisieren Sie die RAM-Disks:

```
update-initramfs -u -k all
```

Starten Sie das System neu.

9. Verwenden Sie unter einem Benutzerkonto mit Root-Rechten die Befehlszeile, um die Setup-Datei auszuführen. Sie können die Installationsdatei von der Kaspersky-Website herunterladen.

   - Um Kaspersky Security Center Web Console zu installieren oder zu aktualisieren, führen Sie den folgenden Befehl aus:

     ```
     sudo apt-get install ksc-web-console-<Build-Nummer>.x86_64.deb
     ```

   - Um eine ältere Version von Kaspersky Security Center Web Console zu aktualisieren, führen Sie den folgenden Befehl aus:

     ```
     sudo apt-get install ksc-web-console-<Build-Nummer>.x86_64.deb
     ```

Dadurch wird die Installationsdatei entpackt. Bitte warten Sie, bis die Installation abgeschlossen ist. Kaspersky Security Center Web Console wird in den folgenden Pfad installiert: `/var/opt/kaspersky/ksc-web-console`.

10. Starten Sie alle Dienste von Kaspersky Security Center Web Console neu. Dazu dient der folgende Befehl:

```
sudo systemctl restart KSC*
```

Nach dem erfolgreichen Abschluss der Installation können Sie in Ihrem Browser Kaspersky Security Center Web Console öffnen und sich einloggen.

Kaspersky Security Center Linux mittels Skript installieren

Mit dem Skript `ksc_fast_install` können Sie Kaspersky Security Center Linux bereitstellen und die Erstkonfiguration folgender Komponenten durchführen: Administrationsserver und Web Console, einschließlich des DBMS und der erforderlichen Support-Pakete.

Das Skript liest Parameter aus der Parameterdatei. Es werden die Standardwerte der Parameter verwendet. Bei Bedarf können Sie die Werte anpassen.

Funktionsweise des Skripts

Das Skript führt die folgenden Schritte durch:

- Prüfen, ob folgende Bedingungen erfüllt sind:
  - Sie verfügen über die erforderlichen Berechtigungen zur Ausführung des Skripts.
  - Das Skript ist mit dem DBMS und dem Betriebssystem kompatibel.
  - Sowohl die EULAs als auch die Datenschutzrichtlinie werden in der Parameterdatei akzeptiert.
  - Die Hardwarevoraussetzungen für den Administrationsserver und die Verteilungspunkte werden erfüllt.

    Die Anforderungen sind im Skalierungshandbuch festgelegt.
- Installieren des DBMS (falls noch nicht installiert) und konfigurieren seiner Parameter
- Erstellen der Datenbanken von Kaspersky Security Center und konfigurieren der Anmeldeinformationen für das Betriebssystem
- Installieren des Administrationsservers und der Web Console
- Bereitstellen des Benutzernamens und Kennworts für die Anmeldung an der Web Console

  Speichern Sie sich diese Anmeldeinformationen auf eine beliebige Weise, bevor Sie das Terminal mit der Befehlszeile schließen. Wenn Sie die Anmeldeinformationen verlieren, müssen Sie ein neues Benutzerkonto hinzufügen, indem Sie den folgenden Befehl ausführen: `` `/opt/kaspersky/ksc64/sbin/kladduser -n <Benutzer>` ``

Wenn eine oder mehrere Bedingungen nicht erfüllt sind oder ein Fehler auftritt, wird das Skript beendet und eine entsprechende Benachrichtigung angezeigt.

Das Skript führt keine Vorgänge zur Systemhärtung durch. Um das Risiko einer Kompromittierung von Kaspersky Security Center zu minimieren, beachten Sie die Empfehlungen des Härtungsleitfadens.
Die skriptbasierte Installation kann zur Bereitstellung von Kaspersky Security Center Linux ab Version 16.3 auf einem Gerät ohne Kaspersky Security Center Linux verwendet werden.
Um das Skript auszuführen, ist Python 3.6 oder höher erforderlich.

Das Skript `ksc_fast_install` unterstützt die Installation von Kaspersky Security Center Linux für die folgenden Versionen der Betriebssysteme und mit folgenden DBMS.

Version des Betriebssystems	DBMS
Ubuntu Server 26.04 LTS	PostgreSQL 18
RED OS 8	PostgreSQL 16
Astra Linux Special Edition RUSB.10015-01 (Version 1.8.5)	PostgreSQL 15
CentOS Stream 10	PostgreSQL 18

So führen Sie die Bereitstellung mittels Skript durch

Erforderliche Vorrausetzungen

Bevor Sie das Skript starten, stellen Sie sicher, dass Sie:

- Mittels des Befehls `dnf update` oder `apt update` Ihr Betriebssystem aktualisiert haben
- Mittels des Befehls `sudo -i` Superuser-Berechtigungen bekommen haben
- Mittels des Befehls `chmod +x ./ksc_fast_install.py` erlaubt haben, dass Skript auszuführen
- Mittels des Befehls `sudo apt policy postgresql` sichergestellt haben, dass sich das unterstützte DBMS im Repository Ihres Betriebssystems befindet

Um Kaspersky Security Center Linux mittels Skripts bereitzustellen, führen Sie die folgenden Schritte durch:

1. Laden Sie von der Kaspersky-Website die folgenden Dateien herunter:
   - Die .deb- oder .rpm-Programmpakete für den Administrationsserver und die Web Console
   - Das Archiv mit dem Skript

     Sie müssen ein Installationsskript verwenden, dessen Version mit der Version von Kaspersky Security Center Linux kompatibel ist, die Sie installieren möchten.

Das Archiv enthält die folgenden Dateien:

- Datei `ksc_fast_install script`
- Parameterdatei

  Der Standardname der Datei ist `params.txt`. Wenn Sie die Datei umbenennen möchten, müssen Sie bei Ausführung des Skripts im Terminal den neuen Dateinamen anhand des Parameters `--params` angeben
- Datei mit der EULA für den Administrationsserver
- Datei mit der EULA für Kaspersky Security Center Web Console
- Datei mit der Datenschutzrichtlinie

2. Legen Sie die heruntergeladenen Dateien im selben lokalen Verzeichnis ab.
3. Konfigurieren Sie bei Bedarf die Parameterdatei.

   Klicken Sie hier, um ein Beispiel für eine Parameterdatei mit Beschreibung der zugehörigen Parameter anzuzeigen

```
# Required parameters:

#klfi_server_eula_accepted=N

#klfi_nwc_eula_accepted=N

#klfi_pp_accepted=N

# Optional parameters:

#klfi_klserver_db=KAV

#klfi_klserver_dbuser=klserver

#klfi_klserver_address=

#klfi_kliam_db=KAV_IAM

#klfi_kliam_dbuser=kliam

#klfi_kliam_address=

#klfi_sys_group_kladmin=kladmins

#klfi_sys_user_klserver=klsrvuser

#klfi_sys_user_kliam=kliamuser

#klfi_sys_user_svc=klsvcuser

#klfi_nwc_port=8080

#klfi_display_name=
```

#klfi_netsize=M

Die Parameter `klfi_server_eula_accepted=N`, `klfi_nwc_eula_accepted=N` und `klfi_pp_accepted=N` sind obligatorisch und immer in der Parameterdatei vorhanden. Die weiteren Parameter sind optional.

Für die obligatorischen Parameter gilt:

- Wenn Sie den Standardwert ändern, ohne die Kommentarzeichen aus einer Zeile zu entfernen, werden Sie aufgefordert, die EULA und die Datenschutzrichtlinie zu akzeptieren.
- Wenn Sie einen anderen Wert als `Y` oder `N` angeben, werden Sie aufgefordert, die EULA und die Datenschutzrichtlinie zu akzeptieren, unabhängig davon, ob Sie die Kommentarzeichen aus der Zeile entfernt haben.
- Wenn Sie die Kommentarzeichen aus der Zeile entfernen, ohne den Standardwert `N` zu ändern, funktioniert das Skript nicht.
- Wenn Sie die Kommentarzeichen aus der Zeile entfernen und den Wert `Y` festlegen, werden Sie vom Skript nicht aufgefordert.

Parameter mit Standardwert	Beschreibung des Parameters und weitere mögliche Werte (falls vorhanden)
`klfi_server_eula_accepted=N`	Endbenutzer-Lizenzvertrag für den Administrationsserver. Mögliche Werte: • `Y` – EULA akzeptiert • `N` – EULA nicht akzeptiert
`klfi_nwc_eula_accepted=N`	Endbenutzer-Lizenzvertrag für Kaspersky Security Center Web Console. Mögliche Werte: • `Y` – EULA akzeptiert • `N` – EULA nicht akzeptiert
`klfi_pp_accepted=N`	Datenschutzrichtlinie. Mögliche Werte: • `Y` – Datenschutzrichtlinie akzeptiert • `N` – Datenschutzrichtlinie nicht akzeptiert
`klfi_klserver_db=KAV`	Name der Datenbank des Administrationsservers. Der Name muss sich von dem Namen der IAM-Datenbank, der in der Variablen `klfi_kliam_db` angegeben ist, unterscheiden.
`klfi_kliam_db=KAV_IAM`	Der Name der IAM-Datenbank. Der Name muss sich von dem Namen der Administrationsserver-Datenbank, der in der Variablen `klfi_klserver_db` angegeben ist, unterscheiden.
`klfi_klserver_dbuser=klserver`	Name des Benutzers der Administrationsserver-Datenbank.
`klfi_kliam_dbuser=kliam`	Name des Benutzers der IAM-Datenbank.
`klfi_klserver_address=FQDN oder Gerätename`	FQDN des Administrationsservers Wenn der Parameterwert nicht angegeben ist, ermittelt das Skript automatisch den FQDN oder den Namen des Geräts, auf dem Sie das Skript ausführen. Wenn das Skript die Werte nicht ermitteln kann, wird die Installation mit einem Fehler abgeschlossen.
`klfi_kliam_address = FQDN oder Gerätename`	FQDN des IAM-Servers. Wenn der Parameterwert nicht angegeben ist, ermittelt das Skript automatisch den FQDN oder den Namen des Geräts, auf dem Sie das Skript ausführen. Wenn das Skript die Werte nicht ermitteln kann, wird die Installation mit einem Fehler abgeschlossen.

`klfi_sys_group_kladmin=kladmins`	Der Name der Sicherheitsgruppe für die Dienste.
`klfi_sys_user_klserver =klsrvuser`	Der Name des Benutzerkontos zum Starten des Administrationsserver-Dienstes.
`klfi_sys_user_kliam =kliamuser`	Der Name des Benutzerkontos zum Starten des IAM-Dienstes.
`klfi_sys_user_svc =klsvcuser`	Der Name des Benutzerkontos zum Starten anderer Dienste.
`klfi_nwc_port=8080`	Port für die Verbindung mit Kaspersky Security Center Web Console.
`klfi_display_name=FQDN`	Der im Login-Fenster anzuzeigende Name des Administrationsservers.
`klfi_netsize=M`	Die ungefähre Anzahl an Geräten, die Sie verwalten möchten: Mögliche Werte: • `S` – 1 bis 1.000 verwaltete Geräte • `M` – 1.000 bis 10.000 verwaltete Geräte • `L` – 10.001 bis 30.000 verwaltete Geräte • `XL` – 30.001 bis 50.000 verwaltete Geräte

Die Zeilen der Parameterdatei sind auskommentiert. Wenn Sie die Werte konfigurieren möchten, entfernen Sie das #-Zeichen am Anfang der Zeile, die Sie aktivieren möchten.

Die Parameter `klfi_server_eula_accepted`, `klfi_nwc_eula_accepted` und `klfi_pp_accepted` sind obligatorisch und ihr Standardwert ist `N`. Wenn Sie das Skript ausführen, ohne diese Werte in der Parameterdatei zu ändern, werden Sie aufgefordert, die EULA und die Datenschutzrichtlinie zu akzeptieren.

4. Führen Sie das Skript aus.

   Nach der Ausführung des Skripts wird eine Benachrichtigung über die erfolgreiche Bereitstellung der Komponenten von Kaspersky Security Center Linux angezeigt. Zusätzlich werden im Terminal der Benutzername und das Kennwort für die Anmeldung an der Web Console ausgegeben.

Wenn die Bedingungen des skriptbasierten Installers nicht erfüllt sind, unbekannte Parameter in der Parameterdatei angegeben sind oder ein Parameter mehrmals wiederholt wird, gibt das Skript einen Fehler zurück und es wird eine entsprechende Benachrichtigung angezeigt.

Wenn bei der Installation der Komponenten von Kaspersky Security Center Linux oder des DBMS ein Fehler auftritt, führt das Skript ein Rollback der Änderungen durch und wird anschließend beendet.

Rollback einer fehlgeschlagenen Installation

Wenn bei der Installation von Kaspersky Security Center Linux oder des DBMS ein Fehler auftritt, führt das Skript automatisch ein Rollback der Änderungen durch. Die vor dem Auftreten des Fehlers installierten Komponenten oder das DBMS werden gelöscht.

Für das Upgrade von Paketen des Betriebssystems und die Installation von unterstützenden Paketen wird kein Rollback ausgeführt.

Wenn Sie das Skript manuell beenden, wird für die erfolgreich abgeschlossenen Schritte kein Rollback ausgeführt. Bei Bedarf können Sie das Skript erneut ausführen und die Installation wird an dem Schritt fortgesetzt, an dem sie unterbrochen wurde.

Um die Installation fortzusetzen, müssen Sie das Skript in der Kommandozeile mit dem Parameter `rollback` starten: `python3 script.py rollback`

Einschränkungen

Für die skriptbasierte Installationsmethode gelten die folgenden Einschränkungen:

- Die Bereitstellung ist nur auf einem Gerät möglich, auf dem kein Kaspersky Security Center Linux installiert ist.

  Ein Upgrade auf eine neue Version von Kaspersky Security Center Linux wird von dem Skript nicht unterstützt.
- Das Skript unterstützt keine benutzerdefinierten Datenbankschemata.
- In den folgenden Fällen können Sie das Skript nicht verwenden:
  - Administrationsserver, Web Console und DBMS werden auf unterschiedlichen Geräten installiert.
  - Das Kaspersky Security Center Linux Failover-Cluster wurde bereitgestellt.
  - Sie verwenden MariaDB Galera Cluster.
  - Sie verwenden einen Postgres-Cluster mit mehreren Cluster-Knoten.

Kaspersky Security Center Linux Failover-Cluster bereitstellen

Ein Kaspersky Security Center Linux Failover-Cluster bietet eine hohe Verfügbarkeit für Kaspersky Security Center Linux und minimiert die Ausfallzeit des Administrationsservers im Falle eines Fehlers. Das Failover-Cluster basiert auf zwei identischen Instanzen von Kaspersky Security Center Linux, die auf zwei Computern installiert sind. Eine der Instanzen arbeitet als aktiver Knoten und die andere ist ein passiver Knoten. Der aktive Knoten verwaltet den Schutz der Client-Geräte, während der passive bereit ist, alle Funktionen des aktiven Knotens zu übernehmen, falls der aktive Knoten ausfällt. Wenn ein Fehler auftritt, wird der passive Knoten aktiv und der aktive Knoten wird passiv.

Das Kaspersky Security Center Linux Failover-Cluster unterstützt zwei Konfigurationen:

- Ein Failover-Cluster, dessen Knoten sich in einem einzelnen Rechenzentrum befinden.
- Ein geografisch verteiltes Failover-Cluster, dessen Knoten sich in verschiedenen Rechenzentren befinden.

In einem Kaspersky Security Center Linux Failover-Cluster werden alle Dienste von Kaspersky Security Center Linux automatisch verwaltet. Versuchen Sie nicht, die Dienste manuell neu zu starten.

Verwenden Sie zur Fehlerbehebung die Syslog-Funktion.

Umschaltbedingungen

Das Failover Cluster schaltet die Verwaltung des Schutzes der Client-Geräte vom aktiven Knoten auf den passiven Knoten um, wenn auf dem aktiven Knoten eines der folgenden Ereignisse auftritt:

- Der aktive Knoten ist aufgrund eines Software- oder Hardwarefehlers defekt.
- Der aktive Knoten wurde für Wartungsaktivitäten vorübergehend gestoppt.

- Mindestens einer der Dienste (oder Prozesse) von Kaspersky Security Center Linux ist fehlgeschlagen oder wurde zufällig beendet. Die Dienste von Kaspersky Security Center Linux bestehen aus: klnagent_klfoc, kladminserver_klfoc, klactprx_klfoc, klwebsrv_klfoc.

- Die Netzwerkverbindung zwischen dem aktiven Knoten und dem Speicher auf dem Dateiserver wurde unterbrochen oder beendet (nur für den Cluster, der sich in einem einzelnen Rechenzentrum befindet).

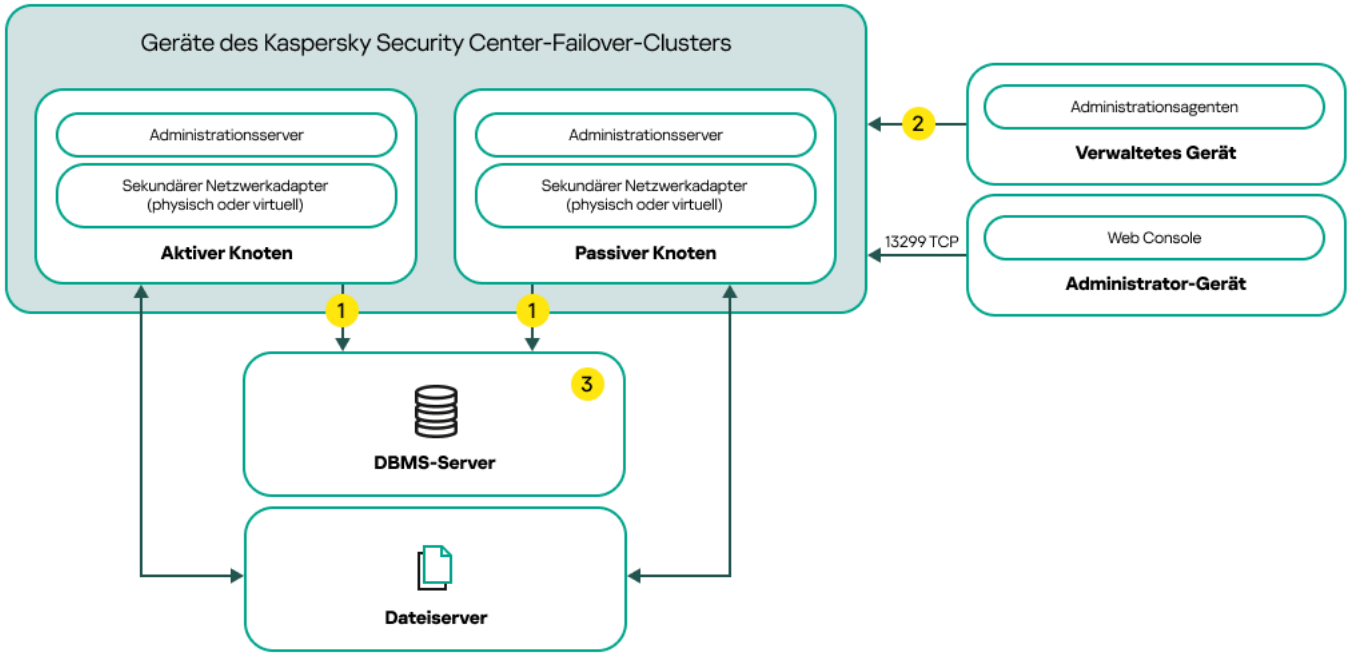
Kaspersky Security Center Linux Failover-Cluster. Bereitstellungsschemata

Für die Bereitstellung des Kaspersky Security Center Linux-Failover-Cluster können Sie aus den folgenden Schemata auswählen:

- Bereitstellung eines Kaspersky Security Center Linux-Failover-Clusters in einem einzelnen Rechenzentrum:
  - Ein Schema, das einen sekundären Netzwerkadapter und ein DBMS verwendet, das auf einem dedizierten Gerät installiert ist
  - Ein Schema, das den Load Balancer eines Drittanbieters und ein DBMS verwendet, das auf einem dedizierten Gerät installiert ist
- Geografisch verteilte Bereitstellung eines Kaspersky Security Center Linux-Failover-Clusters über mehrere Rechenzentren.

Kaspersky Security Center Linux Failover-Cluster

Ein Schema, das einen sekundären Netzwerkadapter und ein DBMS verwendet, das auf einem dedizierten Gerät installiert ist



Ein Schema, das einen sekundären Netzwerkadapter und ein DBMS verwendet, das auf einem dedizierten Gerät installiert ist

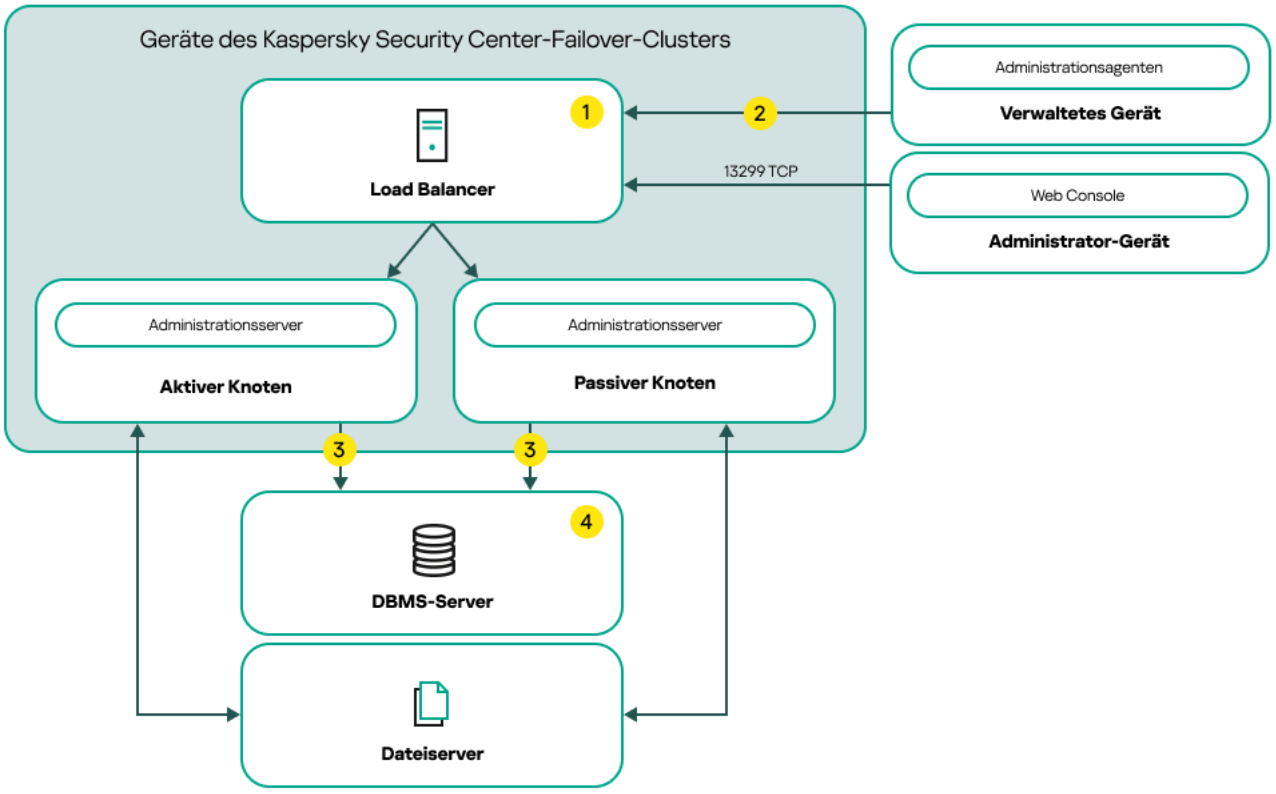
Legende des Schemas:

1 Administrationsserver sendet Daten an die Datenbank. Öffnen Sie auf dem Gerät mit der Datenbank die erforderlichen Ports, z. B. Port 3306 für MySQL Server oder Port 5432 für PostgreSQL oder Postgres Pro. Relevante Informationen finden Sie in der DBMS-Dokumentation.

2 Öffnen Sie auf den Geräten mit dem Administrationsserver die folgenden Ports, um eine Verbindung zu den verwalteten Geräten herzustellen: TCP 13000, UDP 13000 und TCP 17000.

3 Ein Gerät mit Datenbankverwaltungssystem (DBMS). Wenn Sie MariaDB Galera Cluster als DBMS verwenden, ist für diesen Zweck kein dediziertes Gerät erforderlich. Installieren Sie MariaDB Galera Cluster auf jedem der Knoten.

Ein Schema, das den Load Balancer eines Drittanbieters und ein DBMS verwendet, das auf einem dedizierten Gerät installiert ist



Ein Schema, das den Load Balancer eines Drittanbieters und ein DBMS verwendet, das auf einem dedizierten Gerät installiert ist

Legende des Schemas:

1 Öffnen Sie auf dem Gerät des Load-Balancers alle Ports des Administrationsservers: TCP 13000, UDP 13000, TCP 13299 und TCP 17000.

> Wenn Sie das Tool "klakaut" zur Automatisierung verwenden möchten, müssen Sie auch den TCP-Port 13291 öffnen.

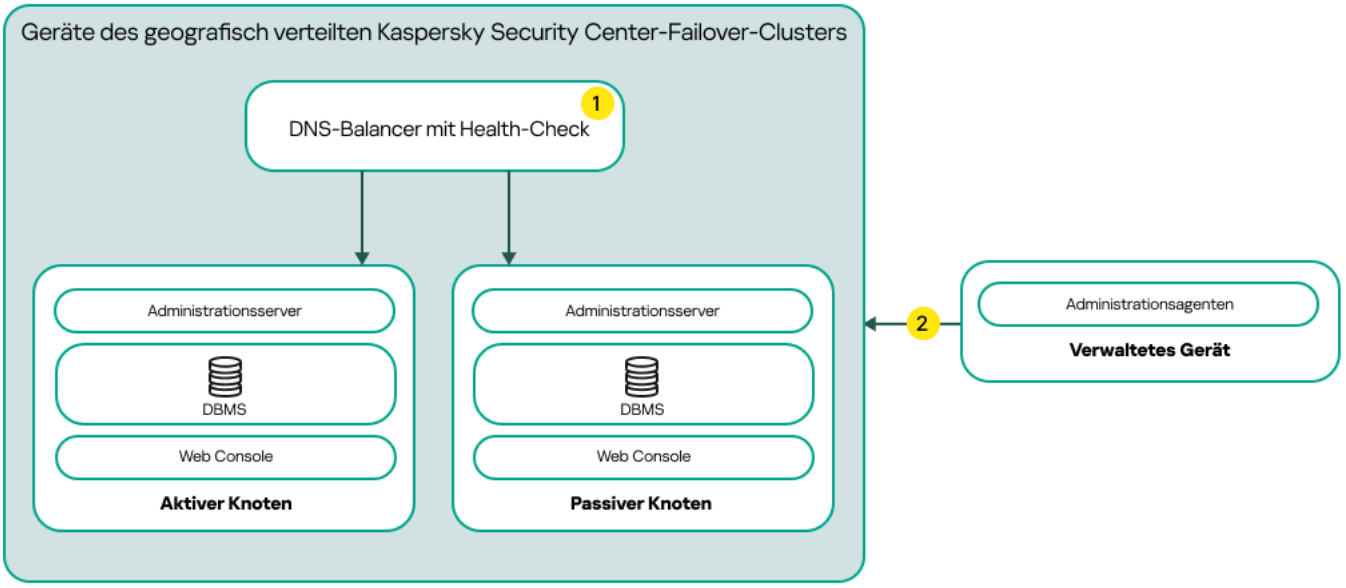
2 Öffnen Sie auf den Geräten mit dem Administrationsserver die folgenden Ports, um eine Verbindung zu den verwalteten Geräten herzustellen: TCP 13000, UDP 13000 und TCP 17000.

3 Administrationsserver sendet Daten an die Datenbank. Öffnen Sie auf dem Gerät mit der Datenbank die erforderlichen Ports, z. B. Port 3306 für MySQL Server oder Port 5432 für PostgreSQL oder Postgres Pro. Relevante Informationen finden Sie in der DBMS-Dokumentation.

4 Ein Gerät mit Datenbankverwaltungssystem (DBMS). Wenn Sie MariaDB Galera Cluster als DBMS verwenden, ist für diesen Zweck kein dediziertes Gerät erforderlich. Installieren Sie MariaDB Galera Cluster auf jedem der Knoten.

Geografisch verteiltes Kaspersky Security Center Linux Failover-Cluster

Dieses Bereitstellungsschema ermöglicht es Ihnen, eine hohe Verfügbarkeit aller Komponenten zu gewährleisten. In diesem Schema werden der Administrationsserver, das DBMS und die Kaspersky Security Center Web Console auf beiden Cluster-Knoten installiert.



Bereitstellungsschema eines geografisch verteilten Kaspersky Security Center Linux Failover-Clusters

1 Bevor das geografisch verteilte Kaspersky Security Center Linux-Failover-Cluster installiert wird, muss ein DNS-Balancer mit Health-Check auf Ihrer Seite bereitgestellt werden.

Der DNS-Balancer überprüft regelmäßig den Status der Cluster-Knoten. Beim Zugriff auf das Cluster über seinen Domänennamen gibt der DNS-Balancer stets die IP-Adresse des aktiven Knotens zurück.

2 Öffnen Sie auf den Geräten mit dem Administrationsserver die folgenden Ports, um eine Verbindung zu den verwalteten Geräten herzustellen: TCP 13000, UDP 13000 und TCP 17000.

Kaspersky Security Center Linux Failover-Cluster

Dieser Abschnitt enthält sowohl allgemeine Informationen über die Bereitstellung eines Kaspersky Security Center Linux Failover-Clusters in einem einzelnen Rechenzentrum als auch Anweisungen zur Vorbereitung und Bereitstellung eines Kaspersky Security Center Linux Failover-Clusters in Ihrem Netzwerk.

Szenario: Kaspersky Security Center Linux Failover-Cluster bereitstellen

Ein Kaspersky Security Center Linux Failover-Cluster bietet eine hohe Verfügbarkeit für Kaspersky Security Center Linux und minimiert die Ausfallzeit des Administrationsservers im Falle eines Fehlers. Das Failover-Cluster basiert auf zwei identischen Instanzen von Kaspersky Security Center Linux, die auf zwei Computern installiert sind. Eine der Instanzen arbeitet als aktiver Knoten und die andere ist ein passiver Knoten. Der aktive Knoten verwaltet den Schutz der Client-Geräte, während der passive bereit ist, alle Funktionen des aktiven Knotens zu übernehmen, falls der aktive Knoten ausfällt. Wenn ein Fehler auftritt, wird der passive Knoten aktiv und der aktive Knoten wird passiv.

Die Bereitstellung von Kaspersky-Anwendungen erfolgt schrittweise:

> Es wird empfohlen, die in diesem Szenario beschriebene Abfolge der Schritte einzuhalten.

1. **Überprüfen der Hardware-Anforderungen**

   Stellen Sie sicher, dass Sie über Hardware verfügen, welche die Anforderungen des Failover Clusters erfüllt.

2. **Auswählen des Bereitstellungsschemas**

   Wählen Sie das Bereitstellungsschema aus. Dies wirkt sich auf die nächsten Schritte der Bereitstellung aus.

3. **Vorbereiten von Benutzerkonten für die Dienste von Kaspersky Security Center Linux**

   Führen Sie die folgenden Schritte auf dem aktiven Knoten, dem passiven Knoten und dem Dateiserver aus:

   1. Erstellen Sie eine Gruppe namens `kladmins`. Führen Sie die folgenden Befehle aus:

      ```
      sudo groupadd kladmins
      ```

      ```
      sudo groupmod -g <neue_GID> kladmins
      ```

      Stellen Sie sicher, dass die Gruppe auf allen drei Geräten dieselbe GID besitzt. Führen Sie den folgenden Befehl aus:

      ```
      getent group kladmins
      ```

      Wenn die GID nicht übereinstimmt, können Sie den folgenden Befehl verwenden, um die GID festzulegen:

      ```
      sudo groupmod -g <neue_GID> kladmins
      ```

   2. Erstellen Sie ein `ksc`-Benutzerkonto. Weisen Sie der Gruppe `kladmins` Benutzerkonten zu. Führen Sie die folgenden Befehle aus:

      ```
      sudo adduser ksc
      ```

      ```
      sudo usermod -u <neue_UID> ksc
      ```

      ```
      sudo gpasswd -a ksc kladmins
      ```

      ```
      sudo usermod -g kladmins ksc
      ```

      Stellen Sie sicher, dass das Benutzerkonto auf allen drei Geräten dieselbe UID besitzt. Führen Sie den folgenden Befehl aus:

      ```
      getent passwd ksc
      ```

      Wenn die UID nicht übereinstimmt, können Sie den folgenden Befehl verwenden, um die UID festzulegen:

      ```
      sudo usermod -u <neue_UID> ksc
      ```

3. Erstellen Sie ein Benutzerkonto `rightless`. Weisen Sie der Gruppe `kladmins` Benutzerkonten zu. Führen Sie die folgenden Befehle aus:

   ```
   sudo adduser rightless
   ```

   ```
   sudo usermod -u <neue_UID> rightless
   ```

   ```
   sudo gpasswd -a rightless kladmins
   ```

   ```
   sudo usermod -g kladmins rightless
   ```

   Stellen Sie sicher, dass das Benutzerkonto auf allen drei Geräten dieselbe UID besitzt. Führen Sie den folgenden Befehl aus:

   ```
   getent passwd rightless
   ```

   Wenn die UID nicht übereinstimmt, können Sie den folgenden Befehl verwenden, um die UID festzulegen:

   ```
   sudo usermod -u <neue_UID> rightless
   ```

4. Erstellen Sie ein `ksciam`-Benutzerkonto. Weisen Sie der Gruppe `kladmins` Benutzerkonten zu. Führen Sie die folgenden Befehle aus:

   ```
   sudo adduser ksciam
   ```

   ```
   sudo usermod -u <neue_UID> ksciam
   ```

   ```
   sudo gpasswd -a ksciam kladmins
   ```

   ```
   sudo usermod -g kladmins ksciam
   ```

   Stellen Sie sicher, dass das Benutzerkonto auf allen drei Geräten dieselbe UID besitzt. Führen Sie den folgenden Befehl aus:

   ```
   getent passwd ksciam
   ```

   Wenn die UID nicht übereinstimmt, können Sie den folgenden Befehl verwenden, um die UID festzulegen:

   ```
   sudo usermod -u <neue_UID> ksciam
   ```

5. Erhöhen Sie bei Bedarf für die Benutzerkonten, die für die Funktionen der Dienste von Kaspersky Security Center Linux verwendet werden, die Anzahl an Dateien, die standardmäßig geöffnet werden können (Datei-Deskriptoren). Öffnen Sie dazu die Datei "/etc/security/limits.conf" und geben Sie die weichen und harten Beschränkungen der Datei-Deskriptoren wie folgt an:

   ```
   ksc soft nofile <max_Anzahl_geöffneter_Dateien>
   ```

   ```
   ksc hard nofile <max_Anzahl_geöffneter_Dateien>
   ```

   Standardmäßig werden die Limits der Datei-Deskriptoren während der Installation angegeben. Die das weiche Datei-Limit beträgt 32.768 und das harte Datei-Limit 131.072 Dateien.

4 Vorbereiten des Dateiservers

Bereiten Sie den Dateiserver darauf vor, als Komponente des Kaspersky Security Center Linux Failover-Clusters zu fungieren. Stellen Sie sicher, dass der Dateiserver die Hardware- und Softwareanforderungen erfüllt, erstellen Sie zwei freigegebene Ordner für die Daten von Kaspersky Security Center Linux und konfigurieren Sie die Berechtigungen für den Zugriff auf die freigegebenen Ordner.

Anleitungen: Einen Dateiservers für das Kaspersky Security Center Linux Failover-Cluster vorbereiten

5 Installation des DBMS

Installieren Sie das DBMS für die Verwendung mit Kaspersky Security Center Linux Sie können eins der unterstützten DBMS verwenden. Informationen zur Installation des ausgewählten DBMS finden Sie in dessen Dokumentation.

Wenn die Distribution Ihres Linux-basierten Betriebssystems ohne unterstütztes DBMS ausgeliefert wird, können Sie das DBMS aus der Paketverwaltung eines Drittanbieters installieren.

Folgen Sie nach der Installation des DBMS der entsprechenden Anweisung:

- PostgreSQL- oder Postgres Pro-Server für die Ausführung mit Kaspersky Security Center Linux konfigurieren
- Den MariaDB x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren

Legen Sie eine Datenbank für IAM an. Der Administrationsserver löscht die IAM-Datenbank nicht automatisch, wenn der Server deinstalliert oder auf ein anderes Gerät verschoben wird. Sie müssen die Datenbank manuell entfernen.

- Für PostgreSQL führen Sie den folgenden Befehl aus:

  `sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"`

- Für MariaDB führen Sie den folgenden Befehl aus:

  `sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"`

Konfigurieren Sie auf dem Gerät mit dem installieren DBMS die Verbindung mit den Geräten, die als aktiver und passiver Knoten fungieren sollen.

6. **Vorbereitung des aktiven und passiven Knotens**

   Bereiten Sie zwei Geräte mit identischer Hardware und Software vor, um als aktiver und passiver Knoten zu fungieren.

   Anleitungen: Knoten für Kaspersky Security Center Linux Failover-Cluster vorbereiten

7. **Installation von Kaspersky Security Center Linux**

   Installieren Sie Kaspersky Security Center Linux im Modus für Failover-Cluster auf beiden Knoten.

   Sie müssen Kaspersky Security Center Linux zunächst auf dem Gerät installieren, das Sie als aktiven Knoten verwenden möchten. Anschließend können Sie es auf dem passiven Knoten installieren.

   Anleitung: So installieren Sie Kaspersky Security Center Linux auf den Knoten des Kaspersky Security Center Linux Failover-Clusters

8. **Installation von Kaspersky Security Center Web Console**

   Installieren Sie Kaspersky Security Center Web Console auf einem separaten Gerät, das kein Knoten eines Clusters ist.

   Geben Sie den Failover-Cluster als Adresse des Administrationsservers in der Antwortdatei an.

   Das Zertifikat des Administrationsservers befindet sich in folgendem Pfad: /mnt/KlFocDataShare_klfoc/1093/cert/klserver.cer

   Kopieren Sie die Zertifikatsdatei auf das Gerät, auf dem die Kaspersky Security Center Web Console installiert wird. Geben Sie den lokalen Pfad des Zertifikats in der Antwortdatei an.

9. **Testen des Failover-Clusters**

   Überprüfen Sie, ob Sie das Failover Cluster richtig konfiguriert haben und ob es ordnungsgemäß funktioniert. Sie können beispielsweise den folgenden Befehl ausführen, um den Wechsel zum passiven Knoten zu initiieren:

   `/opt/kaspersky/ksc64/sbin/klfoc -failover --stp klfoc`

   Verwenden Sie den folgenden Befehl, um zu überprüfen, ob der Verwaltungsdienst des Failover-Clusters auf beiden Knoten den Status `Active: active (running)` besitzt:

   `systemctl status klfocsvc_klfoc`

Verwenden Sie die folgenden Befehle, um zu überprüfen, ob andere Failover-Cluster-Dienste auf dem aktiven Knoten den Status `Active: active (running)` besitzen. Auf dem passiven Knoten müssen diese Failover-Cluster-Dienste stattdessen die Statuswerte `Active: inactive (dead)` oder `Active: failed (Result: signal)` besitzen.

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`
- `systemctl status klwebsrv_klfoc`

Das Kaspersky Security Center Linux Failover-Cluster wurde bereitgestellt.

Kaspersky Security Center Linux Failover-Cluster. Hard- und Softwarevoraussetzungen

Es wird empfohlen, Kaspersky Endpoint Security für Linux auf den aktiven und passiven Knoten, auf dem Gerät mit dem DBMS und auf dem Dateiserver zu installieren. Für die gleichzeitige Installation eines Kaspersky Security Center Linux Failover-Clusters mit Kaspersky Endpoint Security für Linux erhöhen sich die Anforderungen an die Knoten und den Dateiserver um 1,5 GB RAM und 15% CPU-Leistung. Des Weiteren sind mindestens 300 IOPS vorgesehen.

Um ein Kaspersky Security Center Linux Failover-Cluster bereitzustellen, benötigen Sie die folgende Hardware:

- Zwei Geräte mit identischer Hard- und Software. Diese Geräte fungieren als aktiver und passiver Knoten.

  Mindestkonfiguration für aktive und passive Knoten

Hardware	Wert
Prozessor	2 Kerne, 2500 MHz
Arbeitsspeicher	6 GB
Speicherplatz	10 GB, 150 IOPS oder höher
Netzwerkschnittstellen-Controller	1 Gbit/s

- Ein Dateiserver, der das CIFS/SMB-Protokoll ab der Version 2.0 unterstützt. Sie müssen ein dediziertes Gerät bereitstellen, der als Dateiserver fungiert.

  Konfiguration eines Dateiservers

Hardware	Wert
Prozessor	16 Kerne, 2500 MHz
Arbeitsspeicher	32 GB
Speicherplatz	500 GB, 500 IOPS oder höher
Netzwerkschnittstellen-Controller	10 Gbit/s

  Stellen Sie sicher, dass Sie eine hohe Netzwerkbandbreite zwischen dem Dateiserver und den aktiven und passiven Knoten bereitgestellt haben.

- Ein Gerät mit einem Datenbankverwaltungssystem (DBMS). Wenn Sie MariaDB Galera Cluster als DBMS verwenden, ist für diesen Zweck kein dediziertes Gerät erforderlich.

Einen Dateiserver für ein Kaspersky Security Center Linux Failover-Cluster vorbereiten

Der Dateiserver ist eine erforderliche Komponente für das Kaspersky Security Center Linux Failover-Cluster.

So bereiten Sie einen Dateiserver vor:

1. Stellen Sie sicher, dass der Dateiserver die Hardware- und Softwareanforderungen erfüllt.
2. Installieren und konfigurieren Sie einen NFS-Server:
   - Der Zugriff auf den Dateiserver muss für beide Knoten in den NFS-Servereinstellungen aktiviert werden.
   - Das NFS-Protokoll muss die Version 4.0 oder 4.1 haben.
   - Mindestanforderungen für den Linux-Kernel:
     - 3.19.0-25, wenn Sie NFS 4.0 verwenden
     - 4.4.0-176, wenn Sie NFS 4.1 verwenden

   Installieren Sie abhängig von Ihrer Linux-Distribution entweder das Paket "nfs-utils" oder das Paket "nfs-kernel-server", indem Sie den entsprechenden Befehl ausführen:

   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```
3. Erstellen Sie auf dem Dateiserver zwei Ordner und geben Sie diese mithilfe von NFS frei. Einer von ihnen wird verwendet, um Informationen über den Status des Failover-Clusters zu speichern. Der andere dient zum Speichern der Daten und Einstellungen von Kaspersky Security Center Linux. Während der Konfiguration der Installation von Kaspersky Security Center Linux müssen Sie die Pfade zu den freigegebenen Ordnern angeben.

   Stellen Sie sicher, dass die folgenden Ordner nicht existieren:

   - `/mnt/KlFocStateShare`
   - `/mnt/KlFocDataShare_klfoc`

   Wenn einer dieser Ordner bereits existiert, löschen Sie ihn rekursiv.

   Führen Sie die folgenden Befehle aus:

   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   sudo chown ksc:kladmins /mnt/KlFocStateShare
   sudo chown ksc:kladmins /mnt/KlFocDataShare_klfoc
   sudo chmod -R 770 /mnt/KlFocStateShare /mnt/KlFocDataShare_klfoc
   sudo sh -c "echo /mnt/KlFocStateShare *\(rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo sh -c "echo /mnt/KlFocDataShare_klfoc *\
   (rw,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo systemctl start nfs-server
   ```

Aktivieren Sie den Autostart, indem Sie den folgenden Befehl ausführen:

`sudo systemctl enable rpcbind`

Sie können benutzerdefinierte Ordner angeben, es wird jedoch empfohlen, bei Verwendung der Online-Hilfe die vorgeschlagenen Ordnernamen zu verwenden.

4. Starten Sie den Dateiserver neu.

Der Dateiserver ist vorbereitet. Um das Kaspersky Security Center Linux Failover-Cluster bereitzustellen, folgen Sie den weiteren Anweisungen in diesem Szenario.

Knoten für ein Kaspersky Security Center Linux Failover-Cluster vorbereiten

Bevor Sie fortfahren, stellen Sie sicher, dass Sie die vorherigen Schritte im Szenario: Ein Kaspersky-Failover-Cluster bereitstellen ausgeführt haben.

Bereiten Sie zwei Geräte darauf vor, als aktiver und passiver Knoten für das Kaspersky Security Center Linux Failover-Cluster zu fungieren.

Konfiguration der gemeinsamen Ordner

So konfigurieren Sie gemeinsame Ordner:

1. Installieren Sie auf jedem Knoten abhängig von Ihrer Linux-Distribution entweder das Paket "nfs-utils" oder das Paket "nfs-kernel-server", indem Sie den entsprechenden Befehl ausführen:

   `yum install nfs-utils`

   `apt install nfs-kernel-server`

2. Erstellen Sie Einhängepunkte, indem Sie die folgenden Befehle ausführen:

   `mkdir -p /mnt/KlFocStateShare`

   `mkdir -p /mnt/KlFocDataShare_klfoc`

3. Passen Sie die Einhängepunkte und die freigegebenen Ordner an:

   `sudo sh -c "echo <Dateiserver>:/mnt/KlFocStateShare /mnt/KlFocStateShare nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"`

   `sudo sh -c "echo <Dateiserver>:/mnt/KlFocDataShare_klfoc /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"`

   Wobei `{Dateiserver}` der FQDN des Dateiservers mit den freigegebenen Ordnern entspricht.

4. Stellen Sie die freigegebenen Ordner bereit, indem Sie die folgenden Befehle ausführen:

   `mount /mnt/KlFocStateShare`

   `mount /mnt/KlFocDataShare_klfoc`

5. Stellen Sie sicher, dass die Berechtigungen für den Zugriff auf die freigegebenen Ordner ksc:kladmins gehören.

   Führen Sie den folgenden Befehl aus:

   `ls -la /mnt/`

Konfiguration der Netzwerkadapter

Ein sekundärer Netzwerkadapter kann physisch oder virtuell sein. Wenn Sie ein Bereitstellungsschema mit einem sekundären Netzwerkadapter ausgewählt haben, führen Sie das entsprechende Verfahren auf beiden Knoten aus:

- Verwenden Sie einen virtuellen sekundären Netzwerkadapter, der auf einem physischen Netzwerkadapter basiert (MACVLAN-Technologie):

  1. Installieren Sie das Paket iputils-arping. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:

     - `yum install iputils`

     oder

     - `apt install iputils-arping`

  2. Um sicherzustellen, dass NetworkManager zur Verwaltung der physischen Netzwerkadapter verwendet wird, führen Sie den folgenden Befehl aus:

     `nmcli device status`

     Wenn der Befehl ausgibt, dass der physische Netzwerkadapter nicht verwaltet wird, konfigurieren Sie NetworkManager für die Verwaltung des physischen Netzwerkadapters. Die genauen Konfigurationsschritte sind dabei von Ihrer Linux-Distribution abhängig.

  3. Verwenden Sie den folgenden Befehl, um Schnittstellen zu identifizieren:

     `ip a`

  4. Um ein Konfigurationsprofil zu erstellen, führen Sie den folgenden Befehl aus:

     `nmcli connection add type macvlan dev <physische Schnittstelle> mode bridge ifname <virtuelle Schnittstelle> ipv4.addresses <Adressmaske> ipv4.method manual autoconnect no`

- Verwenden Sie einen physischen sekundären Netzwerkadapter oder erstellen Sie ein virtuelles TAP-Gerät mittels eines Hypervisors. Deaktivieren Sie in diesem Szenario das NetworkManager-Tool.

  1. Verbinden Sie den sekundären Netzwerkadapter mit einem Knoten.

  2. Installieren Sie das Paket iputils-arping. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:

     - `yum install iputils`

     oder

     - `apt install iputils-arping`

  3. Um für die Zielschnittstelle die NetworkManager-Verbindung zu löschen, führen Sie den folgenden Befehl aus:

     `nmcli con del <Verbindungsname>`

     Um Verbindungen zu der Zielschnittstelle zu überprüfen, führen Sie den folgenden Befehl aus:

     `nmcli con show`

4. Bearbeiten Sie die Datei "NetworkManager.conf". Suchen Sie den keyfile-Abschnitt und weisen Sie die Zielschnittstelle dem Parameter `unmanaged-devices` zu:

   ```
   [keyfile]
   unmanaged-devices=interface-name:<Name der Schnittstelle>
   ```

5. Starten Sie NetworkManager neu.

   ```
   systemctl reload NetworkManager
   ```

   Um sicherzustellen, dass die Zielschnittstelle nicht mehr verwaltet wird, führen Sie den folgenden Befehl aus:

   ```
   nmcli dev status
   ```

Konfiguration des Load Balancers

Wenn Sie ein Bereitstellungsschema mit Load Balancer ausgewählt haben, folgen Sie den nachstehenden Anweisungen, um es zu konfigurieren.

So konfigurieren Sie den Load Balancer:

1. Bereiten Sie ein separates Linux-Gerät vor, auf dem nginx oder ein anderer Load Balancer installiert ist.
2. Konfigurieren Sie das Load Balancing. Legen Sie den aktiven Knoten als Hauptserver und den passiven Knoten als Backup-Server fest.
3. Öffnen Sie auf dem nginx-Server alle Ports des Administrationsservers gemäß dem folgenden Artikel: Ports, die von Kaspersky Security Center Linux verwendet werden.

Um das Kaspersky Security Center Linux Failover-Cluster bereitzustellen, folgen Sie den weiteren Anweisungen des Szenarios.

> Die Verfügbarkeit der Failover-Cluster-Knoten sollte durch die Verfügbarkeit der hauptsächlichen Verbindungsports zum Administrationsserver bestimmt werden. Der passive Knoten nimmt keine externen Verbindungen an, bis ein Wechsel erfolgt.

Kaspersky Security Center Linux auf den Knoten des Kaspersky Security Center Linux Failover-Clusters installieren

Bevor Sie fortfahren, stellen Sie sicher, dass Sie die vorherigen Schritte im Szenario: Ein Kaspersky-Failover-Cluster bereitstellen ausgeführt haben.

Dieses Verfahren beschreibt die Installation von Kaspersky Security Center Linux auf den Knoten des Kaspersky Security Center Linux Failover-Clusters. Kaspersky Security Center Linux wird auf beiden Knoten des Kaspersky Security Center Linux Failover-Clusters separat installiert. Installieren Sie die Anwendung zunächst auf dem aktiven Knoten und anschließend auf dem passiven. Bei der Installation legen Sie fest, welcher Knoten als aktiv und welcher als passiv fungieren soll.

Abhängig von der auf Ihrem Gerät installierten Linux-Distribution müssen Sie eine der folgenden Installationsdateien verwenden:

- ksc64_[Versionsnummer]_amd64.deb
- ksc64-[Versionsnummer].x86_64.rpm

Die Installationsdatei können Sie von der Kaspersky-Website herunterladen.

Wenn Sie RED OS Version 7.3.4 oder höher bzw. MSVSPHERE Version 9.2 oder höher verwenden, müssen Sie auf beiden Knoten das Paket "libxcrypt-compat" installieren.

Installation auf dem aktiven Knoten

So installieren Sie Kaspersky Security Center Linux auf dem aktiven Knoten:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center Linux installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

2. Wenn Sie einen sekundären Netzwerkadapter verwenden, geben Sie bei Aufforderung dessen Namen ein. Um alle Netzwerkschnittstellen anzuzeigen, können Sie folgenden Befehl eingeben:

   ```
   ip addr
   ```

3. Führen Sie die Installation von Kaspersky Security Center Linux aus. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:

   - `sudo apt-get install /<path>/ksc64_<Versionsnummer>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<Versionsnummer>.x86_64.rpm`

4. Führen Sie die Konfiguration von Kaspersky Security Center Linux aus:

   ```
   /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA) und die Datenschutzrichtlinie. Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie nach der entsprechenden Aufforderung die folgenden Werte ein:

   a. Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren. Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der EULA zustimmen.

   b. Geben Sie `y` ein, wenn Sie die Bedingungen der Datenschutzrichtlinie verstehen und akzeptieren, und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Geben Sie `n` ein, wenn Sie den Bedingungen der Datenschutzrichtlinie nicht zustimmen. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der Datenschutzrichtlinie zustimmen.

6. Wählen Sie **Primärer Cluster-Knoten** als Installationsmodus des Administrationsservers aus.

7. Geben Sie nach der entsprechenden Aufforderung die folgenden Einstellungen an:

   a. Geben Sie den lokalen Pfad zum State Share-Einhängepunkt ein: `/mnt/KlFocStateShare`

   b. Geben Sie den lokalen Pfad zum Data Share-Einhängepunkt ein: `/mnt/KlFocDataShare_klfoc`

   c. Wählen Sie einen Konnektivitätsmodus für das Failover Cluster aus: über einen sekundären Netzwerkadapter oder einen externen Load Balancer.

   d. Wenn Sie einen sekundären Netzwerkadapter verwenden, geben Sie dessen Namen ein.

   e. Geben Sie die FQDN-/IP-Adresse des sekundären Netzwerkadapters oder des externen Load Balancers an.

f. Geben Sie die SSL-Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 13000 festgelegt.

g. Ermitteln Sie die ungefähre Anzahl der Geräte, die Sie verwalten möchten:

- Geben Sie für 1 bis 100 verwaltete Geräte den Wert 1 ein.
- Geben Sie für 101 bis 1.000 verwaltete Geräte den Wert 2 ein.
- Geben Sie für über 1.000 verwaltete Geräte den Wert 3 ein.

Diese Einstellung dient der automatischen, zufälligen Verzögerung von Aufgabenstarts, um die Auslastung auf das Netzwerk zu optimieren. Die folgende Liste enthält die Intervalle, innerhalb denen die Verzögerung berechnet wird:

- 1 bis 100 verwaltete Geräte, Wert 1. Es wird keine Verzögerung verwendet.
- 101 bis 1.000 verwaltete Geräte, Wert 2. Die Verzögerung beträgt 5 Minuten.
- Über 1.000 verwaltete Geräte, Wert 3. Die Verzögerung beträgt 10 Minuten.

h. Geben Sie den Namen der Sicherheitsgruppe für Dienste ein. Standardmäßig wird die Gruppe kladmins verwendet.

i. Geben Sie den Namen des Benutzerkontos ein, um den Administrationsserver-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto "ksc" verwendet.

j. Geben Sie den Namen des Benutzerkontos ein, um andere Dienste zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto "ksc" verwendet.

k. Wählen Sie das DBMS aus, das Sie für die Verwendung mit Kaspersky Security Center Linux installiert haben:

- Wenn Sie MySQL oder MariaDB installiert haben, geben Sie "1" ein.
- Wenn Sie PostgreSQL oder Postgres Pro installiert haben, geben Sie "2" ein.

l. Geben Sie den DNS-Namen oder die IP-Adresse des Gerätes ein, auf dem die Datenbank installiert ist.

m. Geben Sie die Portnummer der Datenbank ein. Dieser Port wird für die Kommunikation mit dem Administrationsserver verwendet. Standardmäßig werden die folgenden Ports verwendet:

- Port 3306 für MySQL oder MariaDB
- Port 5432 für PostgreSQL oder Postgres Pro

n. Geben Sie den Namen der Datenbank ein.

o. Geben Sie den Benutzernamen für das Konto des Datenbank-Administrators ein, das Sie für den Zugriff auf die Datenbank verwenden.

p. Geben Sie das Kennwort für das Konto des Datenbank-Administrators ein, das Sie für den Zugriff auf die Datenbank verwenden.

q. Geben Sie den FQDN des IAM-Servers ein.

Sie müssen den DNS-Name des Administrationsservers angeben, den Sie in Schritt 7e eingegeben haben.

r. Geben Sie den Namen des Kontos ein, um den IAM-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto "ksciam" verwendet.

s. Wählen Sie das DBMS aus, das Sie für die Verwendung des IAM-Dienstes installiert haben:

- Wenn Sie MySQL oder MariaDB installiert haben, geben Sie "1" ein.
- Wenn Sie PostgreSQL oder Postgres Pro installiert haben, geben Sie "2" ein.

t. Geben Sie die Adresse des IAM-DBMS ein, die der IAM-Dienst verwenden soll.

u. Geben Sie die Portnummer des IAM-DBMS ein. Dieser Port wird für die Kommunikation mit dem IAM-Dienst verwendet. Standardmäßig werden die folgenden Ports verwendet:

- Port 3306 für MySQL oder MariaDB
- Port 5432 für PostgreSQL oder Postgres Pro

v. Geben Sie den Namen der IAM-Datenbank ein, den der IAM-Dienst verwenden soll. Der Name der vom IAM-Dienst verwendeten Datenbank muss sich von der Datenbank unterscheiden, die vom Administrationsserver verwendet wird.

w. Geben Sie den Benutzernamen des Datenbank-Benutzerkontos ein, das Sie für den Zugriff auf die IAM-Datenbank verwenden.

x. Geben Sie das Kennwort des Datenbank-Benutzerkontos ein, das Sie für den Zugriff auf die IAM-Datenbank verwenden.

8. Warten Sie, bis die Dienste hinzugefügt und automatisch gestartet wurden:

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc
- kliam_klfoc

9. Erstellen Sie ein Benutzerkonto, das als Administrator des Administrationsservers fungiert. Geben Sie den Benutzernamen und das Kennwort ein. Das Benutzerkennwort muss mindestens 8 Zeichen und darf maximal 256 Zeichen enthalten.

   Wenn Sie diesen Schritt überspringen, können Sie das Konto später mithilfe des folgenden Befehls erstellen:

   `/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <Kennwort>`

Der Benutzer wird hinzugefügt und Kaspersky Security Center Linux wird auf dem primären Knoten installiert.

Installation auf dem sekundären (passiven) Knoten

Um Kaspersky Security Center Linux auf dem sekundären Knoten zu installieren:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center Linux installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.
2. Führen Sie die Installation von Kaspersky Security Center Linux aus. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:
   - `sudo apt-get install /<path>/ksc64_<Versionsnummer>_amd64.deb`
   - `sudo yum install /<path>/ksc64-<Versionsnummer>.x86_64.rpm`
3. Führen Sie die Konfiguration von Kaspersky Security Center Linux aus:

   `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl`
4. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA) und die Datenschutzrichtlinie. Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie nach der entsprechenden Aufforderung die folgenden Werte ein:
   a. Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren. Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der EULA zustimmen.
   b. Geben Sie `y` ein, wenn Sie die Bedingungen der Datenschutzrichtlinie verstehen und akzeptieren, und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Geben Sie `n` ein, wenn Sie den Bedingungen der Datenschutzrichtlinie nicht zustimmen. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der Datenschutzrichtlinie zustimmen.
5. Wählen Sie **Sekundärer Cluster-Knoten** als Installationsmodus des Administrationsservers aus.
6. Geben Sie bei Aufforderung den lokalen Pfad des State Share-Einhängepunkts ein: `/mnt/KlFocStateShare`

Kaspersky Security Center Linux wird auf dem sekundären Knoten installiert.

Überprüfung von Diensten

Verwenden Sie den folgenden Befehl, um zu überprüfen, ob der Verwaltungsdienst des Failover-Clusters den Status `Active: active (running)` besitzt:

```
systemctl status klfocsvc_klfoc
```

Verwenden Sie die folgenden Befehle, um zu überprüfen, ob andere Failover-Cluster-Dienste die Statuswerte `Active: inactive (dead)` besitzen:

- `systemctl status klnagent_klfoc`
- `systemctl status kladminserver_klfoc`
- `systemctl status klactprx_klfoc`

- `systemctl status klwebsrv_klfoc`
- `systemctl status kliam_klfoc`

Sie können jetzt das Kaspersky Security Center Linux Failover-Cluster testen, um sicherzustellen, dass Sie es richtig konfiguriert haben und dass das Cluster ordnungsgemäß funktioniert.

Cluster-Knoten manuell starten und beenden

Möglicherweise müssen Sie das gesamte Kaspersky Security Center Linux Failover-Cluster stoppen oder einen der Cluster-Knoten zu Wartungszwecken vorübergehend trennen. Folgen Sie in diesem Fall den Anweisungen in diesem Abschnitt. Versuchen Sie nicht, die Dienste oder Prozesse im Zusammenhang mit dem Failover-Cluster auf eine andere Weise zu starten oder zu stoppen. Dies kann zu Datenverlust führen.

Starten und Stoppen des gesamten Failover-Clusters zu Wartungszwecken

So starten oder stoppen Sie das gesamten Failover-Cluster:

Führen Sie auf dem aktiven Knoten einen der folgenden Befehle aus:

- Um das Cluster anzuhalten: `/opt/kaspersky/ksc64/sbin/klfoc -stopcluster --stp klfoc`
- Um das Cluster zu starten: `/opt/kaspersky/ksc64/sbin/klfoc -startcluster --stp klfoc`

Das Failover-Cluster wird je nach ausgeführtem Befehl gestartet oder gestoppt.

Wartung eines Knotens

So warten Sie einen der Knoten:

1. Stoppen Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -stopcluster --stp klfoc`.
2. Gehen Sie im Knoten, den Sie verwalten möchten, zu /opt/kaspersky/ksc64/sbin.
3. Öffnen Sie die Befehlszeile und trennen Sie anschließend den Knoten vom Cluster, indem Sie den Befehl `detach_node.sh` ausführen.
4. Starten Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -startcluster --stp klfoc`.
5. Führen Sie die Wartungsarbeiten durch.
6. Stoppen Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -stopcluster --stp klfoc`.
7. Gehen Sie im verwalteten Knoten zu /opt/kaspersky/ksc64/sbin.
8. Öffnen Sie die Befehlszeile und fügen Sie den Knoten anschließend wieder an das Cluster an, indem Sie den Befehl `attach_node.sh` ausführen.

9. Starten Sie auf dem aktiven Knoten das Failover-Cluster mit dem Befehl `klfoc -startcluster --stp klfoc`.

10. Um sicherzustellen, dass der aktuelle Knoten aktiv ist, führen Sie die folgenden Befehle aus, um zu überprüfen, ob die Dienste ausgeführt werden:

    `systemctl status klnagent_klfoc.service`

    `systemctl status kladminserver_klfoc.service`

    `systemctl status klactprx_klfoc.service`

    `systemctl status klwebsrv_klfoc.service`

    `systemctl status kliam_klfoc.service`

    Diese Dienste werden auf dem aktiven Knoten und nicht auf dem passiven Knoten ausgeführt.

Der Knoten ist gewartet und an das Failover-Cluster angehängt.

Knoten eines Failover-Clusters neu installieren

So installieren Sie den Knoten eines Failover-Clusters neu:

1. Erstellen Sie ein Backup des Administrationsservers.

2. Versetzen Sie den aktiven Knoten in den Wartungsmodus.

3. Wenn es erforderlich ist, das aktuelle Betriebssystem beizubehalten, führen Sie die folgenden Schritte aus:

   Wenn Sie vorhaben, das Gerät oder Betriebssystem zu ersetzen, überspringen Sie diesen Schritt.

   a. Um den Failover-Cluster zu stoppen, führen Sie den folgenden Befehl aus:
   `klfoc -stopcluster --stp klfoc`

   b. Um das Stoppen der Dienste des Failover-Clusters zu erzwingen, führen Sie die folgenden Befehle aus:
   `sudo systemctl stop klfocsvc_klfoc`
   `systemctl status kl*klfoc*`

   c. Um die gemounteten Verzeichnisse des Failover-Clusters freizugeben, führen Sie die folgenden Befehle aus:
   `sudo umount /mnt/KlFocDataShare_klfoc`
   `sudo umount /mnt/KlFocStateShare`

   d. Um Kaspersky Security Center Linux zu deinstallieren, führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:

   - `sudo dpkg --remove ksc64`

   oder

   - `sudo yum remove ksc64`

e. Führen Sie für den passiven Knoten alle Schritte der folgenden Anweisungen aus:

1. Knoten für ein Kaspersky Security Center Linux Failover-Cluster vorbereiten.

2. Kaspersky Security Center Linux auf den Knoten des Kaspersky Security Center Linux Failover-Clusters installieren.

4. Beenden Sie den Wartungsmodus. Fahren Sie mit Schritt 6 (Stoppen des Failover-Clusters) der Anleitung Cluster-Knoten manuell starten und beenden fort.

Kaspersky Security Center Web Console mit Verbindung zum Administrationsserver installieren, welcher auf Knoten des Kaspersky Security Center Linux Failover-Clusters bereitgestellt wurde

In diesem Abschnitt wird die Installation des Servers der Web Console von Kaspersky Security Center (im Folgenden auch als "Kaspersky Security Center Web Console" bezeichnet) beschrieben, der eine Verbindung zu dem auf den Knoten des Kaspersky Security Center Linux Failover-Clusters installierten Administrationsserver herstellt. Installieren Sie vor der Installation von Kaspersky Security Center Web Console ein DBMS und Kaspersky Security Center Linux Administration Server auf den Knoten des Kaspersky Security Center Linux Failover-Clusters.

Von der Kaspersky Security Center Web Console werden Installationen auf Cluster-Knoten nicht unterstützt. Es wird empfohlen, die Kaspersky Security Center Web Console auf einem separaten Server zu installieren.

So installieren Sie die Kaspersky Security Center Web Console, die eine Verbindung zu dem auf den Knoten des Kaspersky Security Center Linux Failover-Clusters installierten Administrationsserver herstellt:

1. Führen Sie Schritt 1 und Schritt 2 der Installation von Kaspersky Security Center Web Console aus.

2. Geben Sie in Schritt 3 in der Antwortdatei den Installationsparameter `trusted` an, um der Kaspersky Security Center Web Console die Verbindung mit dem Failover-Cluster von Kaspersky Security Center Linux zu ermöglichen.

   Komponenten des **Installationsparameters** `trusted`

   Wenn Sie für die Verbindung mit einem Kaspersky Security Center Linux Failover-Cluster die Domänenauthentifizierung mit SSO verwenden, geben Sie die vertrauenswürdigen Installationsparameter wie folgt an: Wenn Sie die Kaspersky Security Center Web Console mit einem Administrationsserver der Version 16 oder höher verbinden, wird die durch die Identitäts- und Zugriffsverwaltung (IAM) bereitgestellte Domänenauthentifizierung mit einmaliger Anmeldung (SSO) verwendet. Geben Sie in diesem Fall die Installationsparameter für `trusted` wie folgt an:

```
"trusted":  {
  "<Name des Administrationsservers>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<gemeinsamer Ordner für Daten>/iam/main_certificate.pem",
    "iamPATPath": "<gemeinsamer Ordner für Daten>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<gemeinsamer Ordner für Daten>/1093/cert/klserver.cer"
  }
}
```

wobei:

- `< Name des Administrationsservers >` dem Namen des Kaspersky Security Center Linux Failover-Clusters entspricht, der im Anmeldefenster der Kaspersky Security Center Web Console angezeigt wird.

- `iamHost` der Adresse des Geräts mit installiertem Administrationsserver und IAM entspricht. Wenn Sie im Rahmen der Vorbereitung der Cluster-Knoten einen sekundären Netzwerkadapter erstellt haben, verwenden Sie die FQDN oder den Hostnamen des Adapters als Adresse für das Kaspersky Security Center Linux Failover-Cluster. Geben Sie andernfalls die FQDN oder den Hostnamen des von Ihnen verwendeten Load Balancers eines Drittanbieters an.

  Der Wert `iamHost` muss mit der IAM-Adresse übereinstimmen, die bei der Installation des Administrationsservers angegeben wurde. Um die angegebene IAM-Adresse zu erhalten, führen Sie folgenden Befehl auf dem Host des Administrationsservers aus:

  ```
  grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
  ```

- `iamOAuthPort` dem Port entspricht, der für den Austausch der Authentifizierungstoken über das OpenID Connect-Authentifizierungsprotokoll verwendet wird (der Standardwert beträgt 4444). Dieser Port wird sowohl für die Kommunikation zwischen dem Server der Kaspersky Security Center Web Console und dem Administrationsserver als auch zwischen dem Browser (in dem Kaspersky Security Center Web Console verwendet wird) und dem Administrationsserver verwendet.

- `iamProxyPort` dem Port entspricht, der zur Verbindung des Servers der Kaspersky Security Center Web Console mit dem Administrationsserver verwendet wird (der Standardwert beträgt 9050).

- `iamCertPath` dem Pfad zum IAM-Zertifikat entspricht. Das IAM-Zertifikat wird beim ersten Start des Administrationsservers automatisch erstellt. Die Zertifikatsdatei befindet sich auf dem Gerät, auf dem der Administrationsserver installiert ist. Der Standardpfad des Zertifikats lautet: `< gemeinsamer Ordner für Daten >/iam/main_certificate.pem`. Das Zertifikat befindet sich im freigegebenen Datenspeicher des Kaspersky Security Center Linux Failover-Clusters. Das selbstsignierte IAM-Zertifikat wird automatisch rotiert.

- `iamPATPath` dem Pfad des Tokens entspricht, der für die Registrierung der Kaspersky Security Center Web Console als OAuth-Client in der IAM verwendet wird. Die Datei wird beim ersten Start des Administrationsservers erstellt. Das Token befindet sich auf dem Gerät mit dem installierten Administrationsserver. Der Standardpfad des Tokens lautet: <gemeinsamer Ordner für Daten>/iam/initial_token.txt. Das Token befindet sich im freigegebenen Datenspeicher des Kaspersky Security Center Linux Failover-Clusters. Das Token ist unbegrenzt gültig und erfordert keine Rotation.

- `kscPort` dem OpenAPI-Port entspricht, den Kaspersky Security Center Web Console für die Verbindung mit dem Administrationsserver verwendet (Standardwert ist 13299).

- `kscCertPath` dem Zertifikat des Administrationsservers entspricht, das sich im freigegebenen Datenspeicher des Kaspersky Security Center Linux Failover-Clusters befindet. Der Standardpfad zur Zertifikatsdatei lautet: `< gemeinsamer Ordner für Daten >\1093\cert\klserver.cer`.

  Kopieren Sie Dateien des Zertifikats des Administrationsservers (angegeben durch `kscCertPath`), des IAM-Zertifikats (angegeben durch `iamCertPath`) und des Tokens (angegeben durch `iamPATPath`) vom gemeinsamen Datenspeicher auf das Gerät, auf dem Sie die Kaspersky Security Center Web Console installieren. Geben Sie den lokalen Pfad zum Zertifikat des Administrationsservers an.

Wenn Sie die Kaspersky Security Center Web Console mit einem Administrationsserver der Version 15.4 oder niedriger verbinden, wird die Authentifizierung unter Angabe von Name und Kennwort des Domänenbenutzers oder des internen Benutzers verwendet. Geben Sie in diesem Fall die vertrauenswürdigen Installationsparameter wie folgt an:

```
"trusted":  {
  "<Name des Administrationsservers>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<gemeinsamer Ordner für Daten>/1093/cert/klserver.cer"
  }
}
```

wobei:

- `<Name des Administrationsservers>` dem Namen des Kaspersky Security Center Linux Failover-Clusters entspricht, der im Anmeldefenster der Kaspersky Security Center Web Console angezeigt wird.
- `kscHost` der Adresse (FQDN oder Hostname) des Administrationsservers entspricht. Wenn Sie im Rahmen der Vorbereitung der Cluster-Knoten einen sekundären Netzwerkadapter erstellt haben, verwenden Sie die Adresse des Adapters als Adresse für das Kaspersky Security Center Linux Failover-Cluster. Geben Sie andernfalls die Adresse eines von Ihnen verwendeten Load Balancers eines Drittanbieters an.
- `kscPort` dem OpenAPI-Port entspricht, den Kaspersky Security Center Web Console für die Verbindung mit dem Administrationsserver verwendet (Standardwert ist 13299).
- `kscCertPath` dem Zertifikat des Administrationsservers entspricht, das sich im freigegebenen Datenspeicher des Kaspersky Security Center Linux Failover-Clusters befindet. Der Standardpfad zur Zertifikatsdatei lautet: `<gemeinsamer Ordner für Daten>\1093\cert\klserver.cer`. Kopieren Sie die Zertifikatsdatei aus dem freigegebenen Datenspeicher auf das Gerät, auf dem Sie Kaspersky Security Center Web Console installieren. Geben Sie den lokalen Pfad zum Zertifikat des Administrationsservers an.

3. Fahren Sie mit der standardmäßigen Installationsroutine von Kaspersky Security Center Web Console fort.

Nach dem erfolgreichen Abschluss der Installation können Sie in Ihrem Browser Kaspersky Security Center Web Console öffnen und sich einloggen.

Geografisch verteiltes Kaspersky Security Center Linux Failover-Cluster

Dieser Abschnitt enthält allgemeine Informationen zu geografisch verteilten Kaspersky Security Center Linux-Failover-Clustern sowie Anweisungen zur Vorbereitung und Bereitstellung eines geografisch verteilten Failover-Clusters in Ihrem Netzwerk für die folgenden Konfigurationen:

- Cluster-Knoten mit Ubuntu und PostgreSQL-DBMS
- Cluster-Knoten mit SberLinux und Platform V Pangolin-DBMS

Geografisch verteiltes Cluster mit Ubuntu und PostgreSQL-DBMS

In diesem Szenario wird beschrieben, wie Sie Ihre Infrastruktur auf die Bereitstellung eines geografisch verteilten Kaspersky Security Center Linux-Failover-Clusters vorbereiten.

Erforderliche Vorrausetzungen

- Stellen Sie einen hochverfügbaren DNS-Balancer mit Health-Check bereit.
- Stellen Sie sicher, dass es sich bei den aktiven und passiven Cluster-Knoten um zwei Geräte mit identischer Hardware- und Softwarekonfiguration handelt.
  - Hardwarevoraussetzungen:
    - CPU: 16 Kerne, 2500 MHz
    - RAM: 32 GB
    - Festplattenspeicher: 500 GB bei mindestens 300 IOPS
    - Controller der Netzwerkschnittstelle: 1 Gbps
  - Softwarevoraussetzungen:
    - Betriebssystem: Ubuntu Server 24.04 LTS (Noble Numbat) 64-Bit
    - DBMS: PostgreSQL 17 64-Vit

Schritte

Ein in einem einzelnen Rechenzentrum bereitgestelltes Kaspersky Security Center Linux-Failover-Cluster kann nicht in ein geografisch verteiltes Failover-Cluster transformiert werden.

Die Bereitstellung eines geografisch verteilten Kaspersky Security Center Linux-Failover-Clusters erfolgt in mehreren Schritten:

1. **Vorbereitung des Dateisystems für die Knoten des Failover-Cluster**

   Bereiten Sie das Dateisystem auf beiden Cluster-Knoten vor. Dies umfasst die Erstellung logischer LVM-Volumes und die Konfiguration von Verzeichnissen als Mountpunkte.

2. **Konfiguration eines replizierten Cluster-Dateisystems**

   Installieren Sie die DRBD-Utilities und konfigurieren Sie die DRBD-Ressourcen zur Datenreplikation zwischen den Knoten des Failover-Clusters. Erstellen Sie anschließend auf dem aktiven Cluster-Knoten ein repliziertes Dateisystem.

3. **Installation und Konfiguration von Corosync und Pacemaker auf den Knoten des Failover-Clusters**

   Installieren Sie Corosync und Pacemaker, um die Kommunikation innerhalb des Clusters und die Ressourcenverwaltung für die Hochverfügbarkeit zu gewährleisten.

4. **PostgreSQL-DBMS installieren und konfigurieren**

   Installieren und konfigurieren Sie PostgreSQL auf den Cluster-Knoten.

5. **Installation von Kaspersky Security Center Linux auf den Knoten des Failover-Clusters**

   Installieren Sie Kaspersky Security Center Linux auf den Cluster-Knoten und konfigurieren Sie anschließend die Verschlüsselung zwischen den Knoten.

6. **Installation der Kaspersky Security Center Web Console auf den Knoten des Failover-Clusters**

   Installieren Sie die Kaspersky Security Center Web Console auf beiden Knoten des Failover-Clusters, um Hochverfügbarkeit zu gewährleisten.

Dateisystem der Cluster-Knoten vorbereiten

Als ersten Schritt zur Vorbereitung der Bereitstellung eines geografisch verteilten Kaspersky Security Center Linux-Failover-Clusters müssen Sie auf beiden Cluster-Knoten das Dateisystem einrichten. Dies umfasst die Erstellung logischer LVM-Volumes und die Konfiguration von Verzeichnissen als Mountpunkte. Führen Sie die folgenden Schritte auf beiden Cluster-Knoten aus.

Um das Dateisystem der Cluster-Knoten vorzubereiten:

1. Erstellen Sie ein logisches LVM-Volume für die Daten und die Datenbank des Administrationsservers:

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Erstellen Sie ein separates logisches LVM-Volume zum Speichern der Antwortdatei:

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

   wobei:

   - `volume group name` für den von der LVM verwendeten Gruppennamen des Volumes steht.
   - `klfocdata` und `klfocstate` die logischen Namen der Volumes sind. Diese logischen Volumes werden innerhalb der Volume-Gruppe erstellt.

     Aus Gründen der Konsistenz wird empfohlen, diese Volume-Namen zu verwenden. Sie können bei Bedarf jedoch auch benutzerdefinierte Namen angeben.
   - `volume size` der Größe des Volumes entspricht. Es wird empfohlen, für die Daten und die Datenbank des Administrationsservers mindestens 500 GB einzuplanen. Das Volume für die Antwortdatei benötigt nur wenig Speicherplatz.

2. Erstellen Sie Verzeichnisse, die als Mountpunkte für die logischen Volumes verwendet werden sollen.

   - Für die Daten und die Datenbank des Administrationsservers:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - Für die Antwortdatei:

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

Aus Gründen der Konsistenz wird empfohlen, die Verzeichnisse `/mnt/KlFocDataShare_klfoc` und `/mnt/KlFocStateShare_klfoc` zu verwenden. Bei Bedarf können Sie aber auch benutzerdefinierte Verzeichnisse angeben.

Das Dateisystem der Cluster-Knoten ist vorbereitet. Anschließend müssen Sie ein repliziertes Cluster-Dateisystem konfigurieren.

Eines repliziertes Cluster-Dateisystem vorbereiten

Installation und Konfiguration von DRBD

DRBD ist eine Drittanbietersoftware, die zur Datenreplikation verwendet wird (in diesem Fall für die im vorherigen Schritt vorbereiteten Datenvolumes und Mountpoints).

Nachdem Sie das Dateisystem der Cluster-Knoten vorbereitet haben, müssen Sie DRBD-Utilities installieren und die DRBD-Ressourcen für die Datenreplikation zwischen den Cluster-Knoten konfigurieren. Führen Sie die folgenden Schritte auf beiden Cluster-Knoten aus.

Um DRBD auf einem Cluster-Knoten zu installieren und konfigurieren:

1. Installieren Sie die DRBD-Utilities:

   ```
   apt update
   apt install -y drbd-utils
   ```

   Es wird empfohlen, die DRBD-Version 9.2.6 oder höher zu verwenden, da diese die integrierte Verschlüsselung des Datenverkehrs bietet.

   DRBD-Datenverkehr kann auch mithilfe einer eigenen VPN-Lösung verschlüsselt werden.

2. Erstellen Sie für jedes logische Volume, das während der Vorbereitung des Dateisystems erstellt wurde (`klfocdata` und `klfocstate`) eine Konfigurationsdatei für eine entsprechende DRBD-Ressource.

   Alle Konfigurationsdateien müssen unter `/etc/drbd.d/` abgelegt werden.

   - Ressource `klfocdata` (Daten und Datenbank des Administrationsservers)

     Verwenden Sie für die "klfocdata"-Ressource die asynchrone Replikation ("protocol A"). Konfigurieren Sie alle weiteren Parameter entsprechend Ihrer Umgebung.

     Beispiel für eine Konfigurationsdatei

     ```
     resource klfocdata {
         protocol A;
         net {
             after-sb-0pri    discard-least-changes;
             after-sb-1pri    call-pri-lost-after-sb;
             after-sb-2pri    call-pri-lost-after-sb;
         }
         syncer {
             rate 110M;
         }
         # Hostname of the active node
         on db1 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
         # Hostname of the passive node
         on db2 {
             device    /dev/drbd0;
             disk      /dev/<volume group name>/klfocdata;
             address   <disk IP address>;
             meta-disk internal;
         }
     }
     ```

   - Ressource `klfocstate` (Antwortdatei)

     Um die Ressource "klfocstate" zu erstellen, verwenden Sie die synchrone Replikation ("protocol C"). Konfigurieren Sie alle weiteren Parameter entsprechend Ihrer Umgebung.

Beispiel für eine Konfigurationsdatei

```
resource klfocstate {
    protocol C;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Initialisieren Sie für beide Ressourcen die DRBD-Metadaten:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. DRBD auf allen konfigurierten Ressourcen starten:

```
drbdadm up all
```

DRBD ist auf beiden Cluster-Knoten installiert und konfiguriert.

Erstellen Sie auf dem aktiven Cluster-Knoten ein repliziertes Dateisystem

Nachdem Sie DRBD auf beiden Cluster-Knoten installiert und konfiguriert haben, erstellen Sie auf dem aktiven Cluster-Knoten ein repliziertes Dateisystem. Führen Sie auf dem aktiven Cluster-Knoten die unten beschriebene Schritte aus.

So erstellen Sie ein repliziertes Dateisystem auf dem aktiven Cluster-Knoten:

1. Erhöhen Sie beide DRBD-Ressourcen auf die Rolle "Primary":

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Formatieren Sie die DRBD-Geräte, um die replizierten Volumes für die Verwendung auf den Cluster-Knoten vorzubereiten:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Konfigurieren Sie die Paramter des Dateisystems:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Mounten Sie die DRBD-Geräte in den zuvor erstellten Verzeichnissen:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

   Wenn der multipathd-Dienst installiert ist, muss er so konfiguriert werden, dass er die `/dev/drbd*`-Geräte auf beiden Cluster-Knoten ignoriert.

5. Überprüfen Sie den Status der Replikation:

```
drbdadm status
```

   Die Ausgabe bei einer korrekten Konfiguration des Dateisystems:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Auf dem aktiven Cluster-Knoten ist ein repliziertes Dateisystem konfiguriert. Anschließend müssen Sie Corosync und Pacemaker auf den Cluster-Knoten installieren und konfigurieren.

Corosync und Pacemaker auf den Cluster-Knoten installieren und konfigurieren

Corosync und Pacemaker gewährleisten die Kommunikation innerhalb des Clusters und die Ressourcenverwaltung für die Hochverfügbarkeit. Sie stellen sicher, dass Dienste im Fehlerfall automatisch auf einen funktionierenden Knoten verschoben werden, wodurch Ausfallzeiten minimiert werden.

So installieren und konfigurieren Sie Corosync und Pacemaker auf den Cluster-Knoten:

1. Installieren Sie auf beiden Cluster-Knoten die erforderlichen Pakete:

```
sudo apt install pacemaker -y
sudo apt install crmsh -y
sudo apt install resource-agent-extra -y
```

2. Konfigurieren Sie Corosync und Pacemaker auf beiden Cluster-Knoten entsprechend der offiziellen Dokumentation. Dies umfasst die Aktivierung des Autostarts, die Generierung und Verteilung des Authentifizierungsschlüssels sowie die Konfiguration der Zugriffsberechtigungen für die "authkey"-Datei.

   Um sicherzustellen, dass die Einstellungen korrekt sind, führen Sie auf einem der Cluster-Knoten den folgenden Befehl aus:

```
crm status
```

   Um zu bestätigen, dass Corosync ordnungsgemäß läuft und die Knoten miteinander kommunizieren, sollte die Ausgabe des Befehls den Status des Clusters anzeigen und alle aktiven Knoten auflisten.

3. Konfigurieren Sie auf beiden Cluster-Knoten die grundlegenden Clust-Ereinstellungen für Pacemaker:

```
crm configure property stonith-enabled="false"
crm configure property symmetric-cluster="false"
crm configure rsc_defaults resource-stickiness="110"
crm configure rsc_defaults migration-threshold=3
crm configure property no-quorum-policy=ignore
```

4. Deaktivieren Sie auf beiden Cluster-Knoten den Start von Skripten, die durch Corosync verwaltet werden:

```
systemctl disable drbd.service
```

5. Erstellen Sie auf einem der Cluster-Knoten die DRBD-basierten Ressourcen in Pacemaker.

- DRBD-Ressource für "klfocdata"

  a. Erstellen Sie eine Cluster-Ressource für das DRDB-Volume `klfocdata`, wodurch der Cluster seinen Zustand automatisch verwalten und seine Zustand überwachen kann:

  ```
  crm configure primitive drbd_klfocdata ocf:linbit:drbd params drbd_resource="klfocdata" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Erstellen Sie eine vom Cluster verwaltete Ressource `ms_drbd_klfocdata`, die auf der Ressource `drbd_klfocdata` basiert:

  ```
  crm configure ms ms_drbd_klfocdata drbd_klfocdata meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

  c. Erstellen Sie einen Mountpunkt für das DRBD-Volume `fs_klfocdata`, wobei Sie das Gerät, das Zielverzeichnis, den Typ des Dateisystems und Mount-Optionen angeben müssen:

  ```
  crm configure primitive fs_klfocdata ocf:heartbeat:Filesystem params device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" fstype="ext4" options="data=journal"
  ```

- DRBD resource for klfocstate

  a. Erstellen Sie eine Cluster-Ressource für das DRDB-Volume `klfocstate`, wodurch der Cluster seinen Zustand automatisch verwalten und seine Zustand überwachen kann:

  ```
  crm configure primitive drbd_klfocstate ocf:linbit:drbd params drbd_resource="klfocstate" \
  op monitor interval="60s" op start interval="0" timeout="240s" op stop interval="0" \
  timeout="240s" op monitor role=Master interval="10s" op monitor role=Slave interval="30s"
  ```

  b. Erstellen Sie eine vom Cluster verwaltete Ressource "ms_drbd_klfocstate", die auf der Ressource `drbd_klfocstate` basiert:

  ```
  crm configure ms ms_drbd_klfocstate drbd_klfocstate meta master-max="1" master-node-max="1" \
  clone-max="2" clone-node-max="1" notify="true"
  ```

c. Erstellen Sie einen Mountpunkt für das DRBD-Volume `fs_klfocstate`, wobei Sie das Gerät, das Zielverzeichnis, den Typ des Dateisystems und Mount-Optionen angeben müssen:

```
crm configure primitive fs_klfocstate ocf:heartbeat:Filesystem params device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" fstype="ext4" options="noatime"
```

6. Deaktivieren Sie auf beiden Cluster-Knoten den Autostart des DRBD-Dienstes:

```
systemctl disable drbd.service
```

Corosync und Pacemaker sind auf den Cluster-Knoten installiert und konfiguriert. Anschließend müssen Sie das DBMS installieren und die Administrationsserverdatenbank sowie die IAM-Datenbank erstellen.

PostgreSQL-DBMS installieren und konfigurieren

Nachdem Sie Corosync und Pacemaker auf den Cluster-Knoten installiert und konfiguriert haben, müssen Sie auf beiden Cluster-Knoten das DBMS installieren.

Um das DBMS zu installieren und zu konfigurieren

1. Installieren Sie auf beiden Cluster-Knoten PostgreSQL 17 x64 oder höher.

   Informationen zur Installation eines von PostgreSQL finden Sie in dessen Dokumentation.

2. Stellen Sie sicher, dass auf den Cluster-Knoten mit dem installierten DBMS keine DBMS-Benutzerkonten mit den folgenden Namen vorhanden sind:

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. Stoppen Sie auf beiden ClusterKnoten das DBMS und deaktivieren Sie anschließend den Autotstart des DBMS-Dienstes:

```
sudo systemctl stop postgresql
sudo systemctl disable postgresql
```

4. Kopieren Sie auf dem aktiven Cluster-Knoten das DBMS-Verzeichnis in das Verzeichnis `/mnt/KlFocDataShare_klfoc/dbms`:

```
rsync -av /var/lib/postgresql/17/main/ /mnt/KlFocDataShare_klfoc/dbms
mv /var/lib/postgresql/17/main /var/lib/postgresql/17/main.bk
```

5. Kopieren Sie auf dem aktiven Cluster-Knoten die Konfigurationsdateien von PostgreSQL in das Verzeichnis `/mnt/KlFocDataShare_klfoc/dbms`:

```
sudo cp /etc/postgresql/17/main/pg_hba.conf /mnt/KlFocDataShare_klfoc/dbms
sudo cp /etc/postgresql/17/main/pg_ident.conf /mnt/KlFocDataShare_klfoc/dbms
```

6. Öffnen Sie auf beiden Cluster-Knoten die Konfigurationsdatei `/etc/postgresql/17/main/postgresql.conf` und geben Sie das Verzeichnis `/mnt/KlFocDataShare_klfoc/dbms` als Datenbankverzeichnis an.

   Geben Sie außerdem die Pfade zu den Konfigurationsdateien an (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` und `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) und entfernen Sie den Parameter `include_dir`:

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

7. Öffnen Sie die Konfigurationsdatei `/etc/postgresql/17/main/postgresql.conf` und ändern Sie die DBMS-Konfiguration, sodass sie den Anforderungen von Kaspersky Security Center Linux entspricht.

8. Legen Sie eine Ressource für den PostgreSQL-Dienst an:

```
crm configure primitive klfocsvc_dbms ocf:heartbeat:pgsql \
params pgctl="/usr/lib/postgresql/17/bin/pg_ctl" \
psql="/usr/bin/psql" \
pgdata="/mnt/KlFocDataShare_klfoc/dbms" \
config="/etc/postgresql/17/main/postgresql.conf" \
socketdir="/var/run/postgresql" \
op start timeout=60s \
op stop timeout=60s \
op monitor interval=30s timeout=60s
```

9. Fügen Sie die PostgreSQL-Ressource zur Cluster-Gruppe `group_klfoc` hinzu:

```
crm configure edit klfoc_group
```

10. Fügen Sie am Ende der Liste den Namen der PostgreSQL-Ressource `klfocsvc_dbms` hinzu, zum Beispiel:

```
group klfoc_group {
...
klfocsvc_dbms
}
```

11. Erstellen Sie auf dem DBMS-Server des aktiven Cluster-Knotens eine Datenbank für IAM. Der Name der Datenbank muss sich von dem Namen der Datenbank unterscheiden, die Sie zur Verwendung mit Kaspersky Security Center Linux installiert haben. Der Administrationsserver löscht die IAM-Datenbank nicht automatisch, wenn der Server deinstalliert oder auf ein anderes Gerät verschoben wird. Sie müssen die Datenbank manuell entfernen.

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

Das DBMS ist installiert und konfiguriert. Die Datenbank des Administrationsservers und die IAM-Datenbank wurden erstellt. Anschließend müssen Sie Kaspersky Security Center Linux auf den Cluster-Knoten installieren.

Kaspersky Security Center Linux auf den Knoten eines geografisch verteilten Failover-Clusters installieren

Die Installation von Kaspersky Security Center Linux auf den geografisch verteilten Knoten des Failover-Clusters erfolgt mittels einer Antwortdatei im Silent-Modus (d. h. ohne Benutzereingriff). Die Antwortdatei enthält eine benutzerdefinierte Zusammenstellung von Installationsparametern: Variablen und ihre entsprechenden Werte.

Erforderliche Voraussetzungen

- Führen Sie alle vorbereitenden Schritte durch:
  - Dateisystem aus Cluster-Knoten vorbereiten
  - Eines repliziertes Cluster-Dateisystem vorbereiten
  - Corosync und Pacemaker auf den Cluster-Knoten installieren und konfigurieren
  - PostgreSQL DBMS installieren und konfigurieren
- Stellen Sie sicher, dass auf den Cluster-Knoten Ubuntu Server 24.04 LTS (Noble Numbat) x64 ausgeführt wird.
- Laden Sie die Installationsdatei `ksc64_[version_number]_amd64.deb` von der Kaspersky-Website herunter.

Installation auf dem aktiven Knoten

Um Kaspersky Security Center Linux auf dem aktiven Knoten im Silent-Modus zu installieren:

1. Lesen Sie den Endbenutzer-Lizenzvertrag. Folgen Sie den unten aufgeführten Schritten nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.
2. Erstellen Sie die Gruppe `kladmins` und die nicht-privilegierten Konten `ksc` und `ksciam`, die beide Mitglieder der Gruppe `kladmins` sein müssen. Führen Sie dazu unter einem Benutzerkonto mit Root-Rechten nacheinander die folgenden Befehle aus:

   ```
   adduser ksc
   groupadd kladmins
   gpasswd -a ksc kladmins
   usermod -g kladmins ksc
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

3. Erstellen Sie im Verzeichnis `/mnt/KlFocDataShare_klfoc/` ein Verzeichnis für die Dateien von Kaspersky Security Center Linux:

   ```
   mkdir /mnt/KlFocDataShare_klfoc/ksc/
   ```

4. Erstellen Sie die Antwortdatei (im txt-Format) und fügen Sie der Antwortdatei eine Liste mit Variablen im Format "VARIABLE_NAME=variable_value" hinzu. Verwenden Sie für jede Variable eine separate Zeile.

Geben Sie in der Liste der Parameter, die für die Installation von Kaspersky Security Center Linux im Silent-Modus verwendet werden, die folgenden, zur geografisch verteilten Bereitstellung des Clusters erforderlichen, Parameter an:

- `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

  Geben Sie den Wert `2` an, um das geografisch verteilten Cluster bereitzustellen.

- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` und `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

  Der DNS-Balancer mit Health-Check muss bereits bereitgestellt sein. Die Werte dieser Parameter müssen identisch sein und dem FQDN des DNS-Balancers entsprechen.

5. Geben Sie in der root- oder Benutzerumgebung als Wert für die Umgebungsvariable `KLAUTOANSWERS` den vollständigen Namen der Antwortdatei, einschließlich des enthaltenen Pfades, mit dem folgenden Befehl an:

   ```
   export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
   ```

6. Starten Sie die Installation von Kaspersky Security Center Linux im Silent-Modus, indem Sie die folgenden Befehle ausführen:

   - In der root-Umgebung:

     ```
     apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
     ```

   - In der Benutzerumgebung:

     ```
     sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
     ```

7. Deaktivieren Sie den Autostart des Dienstes "klfocsvc_klfoc.service":

   ```
   systemctl disable klfocsvc_klfoc.service
   ```

8. Stoppen Sie nach der Installation von Kaspersky Security Center Linux den aktiven Cluster-Knoten.

9. Verschieben Sie alle Cluster-Ressourcen auf den passiven Knoten.

   Sie können den Befehl `crm node standby` verwenden (und mittels `crm node online` wieder aufwecken).

Installation auf dem passiven Knoten

Um Kaspersky Security Center Linux auf dem passiven Knoten zu installieren:

1. Starten Sie die Installation von Kaspersky Security Center Linux:

   ```
   sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
   ```

2. Führen Sie die Konfiguration von Kaspersky Security Center Linux aus:

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

3. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA) und die Datenschutzrichtlinie. Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie nach der entsprechenden Aufforderung die folgenden Werte ein:

   - Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren. Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der EULA zustimmen.

   - Geben Sie `y` ein, wenn Sie die Bedingungen der Datenschutzrichtlinie verstehen und akzeptieren, und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Geben Sie "n" ein, wenn Sie die Bedingungen der Datenschutzrichtlinie nicht akzeptieren. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der Datenschutzrichtlinie zustimmen.

4. Wählen Sie den passiven Knoten als Installationsmodus des Administrationsservers aus.

5. Geben Sie auf Aufforderung den lokalen Pfad des State Share-Einhängepunkts ein: `/mnt/KlFocStateShare_klfoc`.

6. Deaktivieren Sie den Autostart des Dienstes "klfocsvc_klfoc.service":

```
systemctl disable klfocsvc_klfoc.service
```

7. Erstellen Sie die Systemressource `klfocsvc_klfoc`:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Fügen Sie die Ressource `klfocsvc_klfoc` der Gruppe `group_klfoc` hinzu:

```
crm configure edit klfoc_group
```

9. Fügen Sie am Ende der Gruppenzeile `klfocsvc_klfoc` hinzu, zum Beispiel:

```
group klfoc_group {
...
klfocsvc_klfoc
}
```

10. Überprüfen Sie, dass sich alle Ressourcen auf dem aktiven Knoten im gestarteten Zustand befinden.

```
crm status
```

Konfigurieren der Verschlüsselung zwischen den Cluster-Knoten

Um die Verschlüsselung zwischen den Cluster-Knoten zu konfigurieren:

Wenn Sie während der Konfiguration des replizierten Cluster-Dateisystems die DRBD-Version 9.2.6 oder höher installiert haben, konfigurieren Sie die Verschlüsselung zwischen den Cluster-Knoten entsprechend der offiziellen DRBD-Dokumentation.

Alternativ können Sie den Datenverkehr zwischen den Cluster-Knoten mithilfe Ihrer eigenen VPN-Lösung verschlüsseln.

Das geografisch verteilte Kaspersky Security Center Linux Failover-Cluster ist installiert. Anschließend müssen Sie die Kaspersky Security Center Web Console auf beiden Cluster-Knoten installieren.

Geografisch verteiltes Cluster mit SberLinux und Platform V Pangolin-DBMS

In diesem Szenario wird beschrieben, wie Sie Ihre Infrastruktur auf die Bereitstellung eines geografisch verteilten Kaspersky Security Center Linux-Failover-Clusters vorbereiten.

Erforderliche Vorrausetzungen

- Stellen Sie einen hochverfügbaren DNS-Balancer mit Health-Check bereit.
- Stellen Sie sicher, dass es sich bei den aktiven und passiven Cluster-Knoten um zwei Geräte mit identischer Hardware- und Softwarekonfiguration handelt.
  - Hardwarevoraussetzungen:
    - CPU: 16 Kerne, 2500 MHz
    - RAM: 32 GB
    - Festplattenspeicher: 500 GB bei mindestens 300 IOPS
    - Controller der Netzwerkschnittstelle: 1 Gbps
  - Softwarevoraussetzungen:
    - Betriebssystem: Platform V SberLinux OS Server (SLO) 9.5.1 64-Bit
    - DBMS: Platform V Pangolin 6.5.1 64-Bit

Schritte

Ein in einem einzelnen Rechenzentrum bereitgestelltes Kaspersky Security Center Linux-Failover-Cluster kann nicht in ein geografisch verteiltes Failover-Cluster transformiert werden.

Die Bereitstellung eines geografisch verteilten Kaspersky Security Center Linux-Failover-Clusters erfolgt in mehreren Schritten:

1. **Vorbereitung des Dateisystems für die Knoten des Failover-Cluster**

   Bereiten Sie das Dateisystem auf beiden Cluster-Knoten vor. Dies umfasst die Erstellung logischer LVM-Volumes und die Konfiguration von Verzeichnissen als Mountpunkte.

2. **Konfiguration eines replizierten Cluster-Dateisystems**

   Installieren Sie die DRBD-Utilities und konfigurieren Sie die DRBD-Ressourcen zur Datenreplikation zwischen den Knoten des Failover-Clusters. Erstellen Sie anschließend auf dem aktiven Cluster-Knoten ein repliziertes Dateisystem.

3. **Installation und Konfiguration von Corosync und Pacemaker auf den Knoten des Failover-Clusters**

   Installieren Sie Corosync und Pacemaker, um die Kommunikation innerhalb des Clusters und die Ressourcenverwaltung für die Hochverfügbarkeit zu gewährleisten.

4. **Installation und Konfiguration des DBMS Platform V Pangolin**

   Installieren und konfigurieren Sie Platform V Pangolin auf den Cluster-Knoten.

5. **Installation von Kaspersky Security Center Linux auf den Knoten des Failover-Clusters**

   Installieren Sie Kaspersky Security Center Linux auf den Cluster-Knoten und konfigurieren Sie anschließend die Verschlüsselung zwischen den Knoten.

6. **Installation der Kaspersky Security Center Web Console auf den Knoten des Failover-Clusters**

   Installieren Sie die Kaspersky Security Center Web Console auf beiden Knoten des Failover-Clusters, um Hochverfügbarkeit zu gewährleisten.

Dateisystem der Cluster-Knoten vorbereiten

Als ersten Schritt zur Vorbereitung der Bereitstellung eines geografisch verteilten Kaspersky Security Center Linux-Failover-Clusters müssen Sie auf beiden Cluster-Knoten das Dateisystem einrichten. Dies umfasst die Erstellung logischer LVM-Volumes und die Konfiguration von Verzeichnissen als Mountpunkte. Führen Sie die folgenden Schritte auf beiden Cluster-Knoten aus.

Um das Dateisystem der Cluster-Knoten vorzubereiten:

1. Erstellen Sie ein logisches LVM-Volume für die Daten und die Datenbank des Administrationsservers:

   ```
   lvcreate -L <volume size> -n klfocdata <volume group name>
   ```

   Erstellen Sie ein separates logisches LVM-Volume zum Speichern der Antwortdatei:

   ```
   lvcreate -L <volume size> -n klfocstate <volume group name>
   ```

wobei:

- `volume group name` für den von der LVM verwendeten Gruppennamen des Volumes steht.
- `klfocdata` und `klfocstate` die logischen Namen der Volumes sind. Diese logischen Volumes werden innerhalb der Volume-Gruppe erstellt.

  Aus Gründen der Konsistenz wird empfohlen, diese Volume-Namen zu verwenden. Sie können bei Bedarf jedoch auch benutzerdefinierte Namen angeben.
- `volume size` der Größe des Volumes entspricht. Es wird empfohlen, für die Daten und die Datenbank des Administrationsservers mindestens 500 GB einzuplanen. Das Volume für die Antwortdatei benötigt nur wenig Speicherplatz.

2. Erstellen Sie Verzeichnisse, die als Mountpunkte für die logischen Volumes verwendet werden sollen.

   - Für die Daten und die Datenbank des Administrationsservers:

     ```
     mkdir -p /mnt/KlFocDataShare_klfoc
     ```

   - Für die Antwortdatei:

     ```
     mkdir -p /mnt/KlFocStateShare_klfoc
     ```

   Aus Gründen der Konsistenz wird empfohlen, die Verzeichnisse `/mnt/KlFocDataShare_klfoc` und `/mnt/KlFocStateShare_klfoc` zu verwenden. Bei Bedarf können Sie aber auch benutzerdefinierte Verzeichnisse angeben.

Das Dateisystem der Cluster-Knoten ist vorbereitet. Anschließend müssen Sie ein repliziertes Cluster-Dateisystem konfigurieren.

Eines repliziertes Cluster-Dateisystem vorbereiten

Installation und Konfiguration von DRBD

DRBD ist eine Drittanbietersoftware, die zur Datenreplikation verwendet wird (in diesem Fall für die im vorherigen Schritt vorbereiteten Datenvolumes und Mountpoints).

Nachdem Sie das Dateisystem der Cluster-Knoten vorbereitet haben, müssen Sie DRBD-Utilities installieren und die DRBD-Ressourcen für die Datenreplikation zwischen den Cluster-Knoten konfigurieren. Führen Sie die folgenden Schritte auf beiden Cluster-Knoten aus.

Um DRBD auf einem Cluster-Knoten zu installieren und konfigurieren:

1. Installieren Sie die DRBD-Utilities wie folgt:

   a. Aktivieren Sie auf beiden Knoten die EPEL- und ELRepo-Repositories:

   ```
   dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   dnf install https://www.elrepo.org/elrepo-release-9.el9.elrepo.noarch.rpm
   ```

b. Geben Sie alle verfügbaren Versionen des kmod-drbd9x-Pakets aus und filtern Sie die Paketliste nach der Plattform "el9_6" (z. B. wird Platform V SberLinux OS Server (SLO) 9.6 verwendet):

```
dnf search --showduplicates kmod-drbd9x | grep el9_6
```

c. Installieren Sie auf beiden Knoten die aktuellste verfügbare Version aus der Liste. Beispiel für Platform V SberLinux OS Server (SLO) 9.6:

```
dnf install kmod-drbd9x-9.2.14-1.el9_6.elrepo.x86_64
dnf install drbd drbd-utils drbd-udev drbd-pacemaker drbd-selinux
modprobe drbd
```

Sollte eine aktuellere Version verfügbar sein, ersetzen Sie die Versionszeichenfolge entsprechend.

Es wird empfohlen, die DRBD-Version 9.2.6 oder höher zu verwenden, da diese die integrierte Verschlüsselung des Datenverkehrs bietet.

DRBD-Datenverkehr kann auch mithilfe einer eigenen VPN-Lösung verschlüsselt werden.

2. Erstellen Sie für jedes logische Volume, das während der Vorbereitung des Dateisystems erstellt wurde (`klfocdata` und `klfocstate`) eine Konfigurationsdatei für eine entsprechende DRBD-Ressource.

   Alle Konfigurationsdateien müssen unter `/etc/drbd.d/` abgelegt werden.

   - Ressource `klfocdata` (Daten und Datenbank des Administrationsservers)

     Verwenden Sie für die "klfocdata"-Ressource die asynchrone Replikation ("protocol A"). Konfigurieren Sie alle weiteren Parameter entsprechend Ihrer Umgebung.

     Beispiel für eine Konfigurationsdatei

```
resource klfocdata {
    protocol A;
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd0;
        disk      /dev/<volume group name>/klfocdata;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

   - Ressource `klfocstate` (Antwortdatei)

     Um die Ressource "klfocstate" zu erstellen, verwenden Sie die synchrone Replikation ("protocol C"). Konfigurieren Sie alle weiteren Parameter entsprechend Ihrer Umgebung.

     Beispiel für eine Konfigurationsdatei

```
resource klfocstate {
    protocol C;
```

```
    net {
        after-sb-0pri    discard-least-changes;
        after-sb-1pri    call-pri-lost-after-sb;
        after-sb-2pri    call-pri-lost-after-sb;
    }
    syncer {
        rate 110M;
    }
    # Hostname of the active node
    on db1 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
    # Hostname of the passive node
    on db2 {
        device    /dev/drbd2;
        disk      /dev/<volume group name>/klfocstate;
        address   <disk IP address>;
        meta-disk internal;
    }
}
```

3. Initialisieren Sie für beide Ressourcen die DRBD-Metadaten:

```
drbdadm create-md klfocdata
drbdadm create-md klfocstate
```

4. DRBD auf allen konfigurierten Ressourcen starten:

```
drbdadm up all
```

DRBD ist auf beiden Cluster-Knoten installiert und konfiguriert.

Erstellen Sie auf dem aktiven Cluster-Knoten ein repliziertes Dateisystem

Nachdem Sie DRBD auf beiden Cluster-Knoten installiert und konfiguriert haben, erstellen Sie auf dem aktiven Cluster-Knoten ein repliziertes Dateisystem. Führen Sie auf dem aktiven Cluster-Knoten die unten beschriebene Schritte aus.

So erstellen Sie ein repliziertes Dateisystem auf dem aktiven Cluster-Knoten:

1. Erhöhen Sie beide DRBD-Ressourcen auf die Rolle "Primary":

```
drbdadm primary --force klfocdata
drbdadm primary --force klfocstate
```

2. Formatieren Sie die DRBD-Geräte, um die replizierten Volumes für die Verwendung auf den Cluster-Knoten vorzubereiten:

```
mkfs.ext4 /dev/drbd0
mkfs.ext4 /dev/drbd2
```

3. Konfigurieren Sie die Paramter des Dateisystems:

```
tune2fs -m 0 /dev/drbd0
tune2fs -m 0 /dev/drbd2
```

4. Mounten Sie die DRBD-Geräte in den zuvor erstellten Verzeichnissen:

```
mount -o noatime /dev/drbd0 /mnt/KlFocDataShare_klfoc
mount -o noatime /dev/drbd2 /mnt/KlFocStateShare_klfoc
```

   Wenn der multipathd-Dienst installiert ist, muss er so konfiguriert werden, dass er die `/dev/drbd*`-Geräte auf beiden Cluster-Knoten ignoriert.

5. Überprüfen Sie den Status der Replikation:

```
drbdadm status
```

   Die Ausgabe bei einer korrekten Konfiguration des Dateisystems:

```
klfocdata role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate

klfocstate role:Secondary
disk:UpToDate open:no
db2 role:Primary tls:yes
peer-disk:UpToDate
```

Auf dem aktiven Cluster-Knoten ist ein repliziertes Dateisystem konfiguriert. Anschließend müssen Sie Corosync und Pacemaker auf den Cluster-Knoten installieren und konfigurieren.

Corosync und Pacemaker auf den Cluster-Knoten installieren und konfigurieren

Corosync und Pacemaker gewährleisten die Kommunikation innerhalb des Clusters und die Ressourcenverwaltung für die Hochverfügbarkeit. Sie stellen sicher, dass Dienste im Fehlerfall automatisch auf einen funktionierenden Knoten verschoben werden, wodurch Ausfallzeiten minimiert werden.

So installieren und konfigurieren Sie Corosync und Pacemaker auf den Cluster-Knoten:

1. Installieren Sie auf beiden Cluster-Knoten die erforderlichen Pakete:

```
dnf install pcs
dnf install drbd-pacemaker
```

2. Konfigurieren Sie Corosync und Pacemaker auf beiden Cluster-Knoten entsprechend der offiziellen Dokumentation. Dies umfasst die Aktivierung des Autostarts, die Generierung und Verteilung des Authentifizierungsschlüssels sowie die Konfiguration der Zugriffsberechtigungen für die "authkey"-Datei.

   Um sicherzustellen, dass die Einstellungen korrekt sind, führen Sie auf einem der Cluster-Knoten den folgenden Befehl aus:

```
crm status
```

   Um zu bestätigen, dass Corosync ordnungsgemäß läuft und die Knoten miteinander kommunizieren, sollte die Ausgabe des Befehls den Status des Clusters anzeigen und alle aktiven Knoten auflisten.

3. Konfigurieren Sie auf beiden Cluster-Knoten die grundlegenden Clust-Ereinstellungen für Pacemaker:

```
pcs property set stonith-enabled=false
pcs property set symmetric-cluster=false
pcs resource defaults resource-stickiness=110
pcs resource defaults migration-threshold=3
pcs property set no-quorum-policy=ignore
```

4. Deaktivieren Sie auf beiden Cluster-Knoten den Start von Skripten, die durch Corosync verwaltet werden:

```
systemctl disable drbd.service
```

5. Erstellen Sie auf einem der Cluster-Knoten die DRBD-basierten Ressourcen in Pacemaker.

- DRBD-Ressource für "klfocdata"

  a. Erstellen Sie eine Cluster-Ressource für das DRDB-Volume `klfocdata`, wodurch der Cluster seinen Zustand automatisch verwalten und seine Zustand überwachen kann:

  ```
  pcs resource create drbd_klfocdata ocf:linbit:drbd \
  drbd_resource="klfocdata" \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Master interval=10s \
  op monitor role=Slave interval=30s \
  ```

  b. Erstellen Sie eine vom Cluster verwaltete Ressource `ms_drbd_klfocdata`, die auf der Ressource `drbd_klfocdata` basiert:

  ```
  pcs resource clone drbd_klfocdata promotable=true
  master-max=1
  clone-max=2
  clone-node-max=1 notify=true
  ```

  c. Erstellen Sie einen Mountpunkt für das DRBD-Volume `fs_klfocdata`, wobei Sie das Gerät, das Zielverzeichnis, den Typ des Dateisystems und Mount-Optionen angeben müssen:

  ```
  pcs resource create fs_klfocdata ocf:heartbeat:Filesystem \
  device="/dev/drbd0" \
  directory="/mnt/KlFocDataShare_klfoc" \
  fstype="ext4" \
  options="data=journal"
  ```

- DRBD resource for klfocstate

  a. Erstellen Sie eine Cluster-Ressource für das DRDB-Volume `klfocstate`, wodurch der Cluster seinen Zustand automatisch verwalten und seine Zustand überwachen kann:

  ```
  pcs resource create drbd_klfocstate ocf:linbit:drbd \
  drbd_resource=klfocstate \
  op monitor interval=60s \
  op start interval=0 timeout=240s \
  op stop interval=0 timeout=240s \
  op monitor role=Promoted interval=10s \
  op monitor role=Unpromoted interval=30s \
  ```

b. Erstellen Sie eine vom Cluster verwaltete Ressource "ms_drbd_klfocstate", die auf der Ressource `drbd_klfocstate` basiert:

```
pcs resource clone drbd_klfocstate promotable=true \
master-max=1 \
clone-max=2 \
clone-node-max=1 \
notify=true
```

c. Erstellen Sie einen Mountpunkt für das DRBD-Volume `fs_klfocstate`, wobei Sie das Gerät, das Zielverzeichnis, den Typ des Dateisystems und Mount-Optionen angeben müssen:

```
pcs resource create fs_klfocstate ocf:heartbeat:Filesystem \
device="/dev/drbd2" \
directory="/mnt/KlFocStateShare_klfoc" \
fstype="ext4" \
options="noatime"
```

6. Deaktivieren Sie auf beiden Cluster-Knoten den Autostart des DRBD-Dienstes:

```
systemctl disable drbd.service
```

Corosync und Pacemaker sind auf den Cluster-Knoten installiert und konfiguriert. Anschließend müssen Sie das DBMS installieren und die Administrationsserverdatenbank sowie die IAM-Datenbank erstellen.

Installation und Konfiguration des DBMS Platform V Pangolin

Nachdem Sie Corosync und Pacemaker auf den Cluster-Knoten installiert und konfiguriert haben, müssen Sie auf beiden Cluster-Knoten das DBMS installieren.

Um das DBMS zu installieren und zu konfigurieren

1. Installieren Sie auf beiden Cluster-Knoten Platform V Pangolin 6.5.1 x64 oder höher.

   Informationen zur Installation eines von Platform V Pangolin finden Sie in dessen Dokumentation.

2. Stellen Sie sicher, dass auf den Cluster-Knoten mit dem installierten DBMS keine DBMS-Benutzerkonten mit den folgenden Namen vorhanden sind:

   - client
   - iam
   - ksc
   - locker
   - pat
   - scope
   - voltron

3. Kopieren Sie auf dem aktiven Cluster-Knoten das DBMS-Verzeichnis in das Verzeichnis `/mnt/KlFocDataShare_klfoc/dbms`:

```
sudo rsync -av  /pgdata/06/data/ /mnt/KlFocDataShare_klfoc/dbms
sudo mv /pgdata/06/data/ /pgdata/06/data.bk/
```

4. Öffnen Sie auf beiden Cluster-Knoten die Konfigurationsdatei `/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf` und geben Sie das Verzeichnis `/mnt/KlFocDataShare_klfoc/dbms` als Datenbankverzeichnis an.

   Geben Sie außerdem die Pfade zu den Konfigurationsdateien an (`/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf` und `/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf`) und entfernen Sie den Parameter `include_dir`:

```
data_directory = '/mnt/KlFocDataShare_klfoc/dbms'
hba_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_hba.conf'
ident_file = '/mnt/KlFocDataShare_klfoc/dbms/pg_ident.conf'
listen_addresses = '*'
```

5. Legen Sie eine Ressource für den DBMS-Dienst an.

```
pcs resource create klfocsvc_dbms pgsql \
pgctl="/usr/pangolin-6.5/bin/pg_ctl"  psql="/usr/bin/psql" pgdata="/mnt/KlFocDataShare_klfoc/dbms"
config="/mnt/KlFocDataShare_klfoc/dbms/postgresql.conf" socketdir="/tmp" \
op start timeout=60s interval=0s \
op stop timeout=60s interval=0s \
op monitor interval=30s timeout=60s \
op promote timeout=120s interval=0s \
op demote timeout=120s interval=0s \
meta target-role=Started
```

6. Deaktivieren Sie auf beiden Cluster-Knoten den Autostart des DBMS-Dienstes:

```
sudo systemctl disable pangolin.service
```

7. Fügen Sie die DBMS-Ressource `klfocsvc_dbms` zur Cluster-Gruppe `group_klfoc` hinzu:

```
pcs resource group add group_klfoc klfocsvc_dbms
```

8. Fügen Sie am Ende der Liste den Namen der DBMS-Ressource `klfocsvc_dbms` hinzu, zum Beispiel:

```
group klfoc_group {
...
klfocsvc_dbms
}
```

9. Erstellen Sie auf dem DBMS-Server des aktiven Cluster-Knotens eine Datenbank für IAM. Der Name der Datenbank muss sich von dem Namen der Datenbank unterscheiden, die Sie zur Verwendung mit Kaspersky Security Center Linux installiert haben. Der Administrationsserver löscht die IAM-Datenbank nicht automatisch, wenn der Server deinstalliert oder auf ein anderes Gerät verschoben wird. Sie müssen die Datenbank manuell entfernen.

```
sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
```

Das DBMS ist installiert und konfiguriert. Die Datenbank des Administrationsservers und die IAM-Datenbank

wurden erstellt. Anschließend müssen Sie Kaspersky Security Center Linux auf den Cluster-Knoten installieren.

Kaspersky Security Center Linux auf den Knoten eines geografisch verteilten Failover-Clusters installieren

Die Installation von Kaspersky Security Center Linux auf den geografisch verteilten Knoten des Failover-Clusters erfolgt mittels einer Antwortdatei im Silent-Modus (d. h. ohne Benutzereingriff). Die Antwortdatei enthält eine benutzerdefinierte Zusammenstellung von Installationsparametern: Variablen und ihre entsprechenden Werte.

Erforderliche Voraussetzungen

- Führen Sie alle vorbereitenden Schritte durch:
  - Dateisystem aus Cluster-Knoten vorbereiten
  - Eines repliziertes Cluster-Dateisystem vorbereiten
  - Corosync und Pacemaker auf den Cluster-Knoten installieren und konfigurieren
  - Installation und Konfiguration des DBMS Platform V Pangolin
- Stellen Sie sicher, dass auf den Cluster-Knoten Platform V SberLinux OS Server (SLO) 9.5.1 x64 ausgeführt wird.
- Laden Sie die Installationsdatei `ksc64_[version_number]_amd64.deb` von der Kaspersky-Website herunter.

Installation auf dem aktiven Knoten

Um Kaspersky Security Center Linux auf dem aktiven Knoten im Silent-Modus zu installieren:

1. Lesen Sie den Endbenutzer-Lizenzvertrag. Folgen Sie den unten aufgeführten Schritten nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.
2. Erstellen Sie die Gruppe `kladmins` und die nicht-privilegierten Konten `ksc` und `ksciam`, die beide Mitglieder der Gruppe `kladmins` sein müssen. Führen Sie dazu unter einem Benutzerkonto mit Root-Rechten nacheinander die folgenden Befehle aus:

   ```
   adduser ksc
   groupadd kladmins
   gpasswd -a ksc kladmins
   usermod -g kladmins ksc
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

3. Erstellen Sie im Verzeichnis `/mnt/KlFocDataShare_klfoc/` ein Verzeichnis für die Dateien von Kaspersky Security Center Linux:

   ```
   mkdir /mnt/KlFocDataShare_klfoc/ksc/
   ```

4. Erstellen Sie die Antwortdatei (im txt-Format) und fügen Sie der Antwortdatei eine Liste mit Variablen im Format "VARIABLE_NAME=variable_value" hinzu. Verwenden Sie für jede Variable eine separate Zeile.

Geben Sie in der Liste der Parameter, die für die Installation von Kaspersky Security Center Linux im Silent-Modus verwendet werden, die folgenden, zur geografisch verteilten Bereitstellung des Clusters erforderlichen, Parameter an:

- `KLFOC_UNATT_EXT_RESOURCE_MANAGEMENT=2`

  Geben Sie den Wert `2` an, um das geografisch verteilten Cluster bereitzustellen.

- `KLSRV_UNATT_SERVERADDRESS=<DNS balancer address>` und `KLSRV_UNATT_IAM_ADDRESS=<DNS balancer address>`

  Der DNS-Balancer mit Health-Check muss bereits bereitgestellt sein. Die Werte dieser Parameter müssen identisch sein und dem FQDN des DNS-Balancers entsprechen.

5. Geben Sie in der root- oder Benutzerumgebung als Wert für die Umgebungsvariable `KLAUTOANSWERS` den vollständigen Namen der Antwortdatei, einschließlich des enthaltenen Pfades, mit dem folgenden Befehl an:

```
export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
```

6. Starten Sie die Installation von Kaspersky Security Center Linux im Silent-Modus, indem Sie die folgenden Befehle ausführen:

   - In der root-Umgebung:

```
apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

   - In der Benutzerumgebung:

```
sudo -E apt-get install /<path>/ksc64_[version_number]_amd64.deb -y
```

7. Deaktivieren Sie den Autostart des Dienstes "klfocsvc_klfoc.service":

```
systemctl disable klfocsvc_klfoc.service
```

8. Stoppen Sie nach der Installation von Kaspersky Security Center Linux den aktiven Cluster-Knoten.

9. Verschieben Sie alle Cluster-Ressourcen auf den passiven Knoten.

   Sie können den Befehl `pcs node standby` verwenden (und mittels `pcs node online` wieder aufwecken).

Installation auf dem passiven Knoten

Um Kaspersky Security Center Linux auf dem passiven Knoten zu installieren:

1. Starten Sie die Installation von Kaspersky Security Center Linux:

```
sudo apt-get install /<path>/ksc64_<version_number>_amd64.deb
```

2. Führen Sie die Konfiguration von Kaspersky Security Center Linux aus:

```
/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

3. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA) und die Datenschutzrichtlinie. Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie nach der entsprechenden Aufforderung die folgenden Werte ein:

   - Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren. Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der EULA zustimmen.

   - Geben Sie `y` ein, wenn Sie die Bedingungen der Datenschutzrichtlinie verstehen und akzeptieren, und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist. Geben Sie "n" ein, wenn Sie die Bedingungen der Datenschutzrichtlinie nicht akzeptieren. Um Kaspersky Security Center Linux zu nutzen, müssen Sie den Bestimmungen der Datenschutzrichtlinie zustimmen.

4. Wählen Sie den passiven Knoten als Installationsmodus des Administrationsservers aus.

5. Geben Sie auf Aufforderung den lokalen Pfad des State Share-Einhängepunkts ein: `/mnt/KlFocStateShare_klfoc`.

6. Deaktivieren Sie den Autostart des Dienstes "klfocsvc_klfoc.service":

```
systemctl disable klfocsvc_klfoc.service
```

7. Erstellen Sie die Systemressource `klfocsvc_klfoc`:

```
crm configure primitive klfocsvc_klfoc systemd:klfocsvc_klfoc \
op start timeout="900s" interval="0" \
op stop timeout="900s" interval="0" \
op monitor interval="30s" timeout="90s"
```

8. Fügen Sie die Ressource `klfocsvc_klfoc` der Gruppe `group_klfoc` hinzu:

```
pcs resource group add group_klfoc klfocsvc_klfoc
```

9. Fügen Sie am Ende der Gruppenzeile `klfocsvc_klfoc` hinzu, zum Beispiel:

```
group klfoc_group {
...
klfocsvc_klfoc
}
```

10. Überprüfen Sie, dass sich alle Ressourcen auf dem aktiven Knoten im gestarteten Zustand befinden.

```
pcs status
```

Konfigurieren der Verschlüsselung zwischen den Cluster-Knoten

Um die Verschlüsselung zwischen den Cluster-Knoten zu konfigurieren:

Wenn Sie während der Konfiguration des replizierten Cluster-Dateisystems die DRBD-Version 9.2.6 oder höher installiert haben, konfigurieren Sie die Verschlüsselung zwischen den Cluster-Knoten entsprechend der offiziellen DRBD-Dokumentation.

Alternativ können Sie den Datenverkehr zwischen den Cluster-Knoten mithilfe Ihrer eigenen VPN-Lösung verschlüsseln.

Das geografisch verteilte Kaspersky Security Center Linux Failover-Cluster ist installiert. Anschließend müssen Sie die Kaspersky Security Center Web Console auf beiden Cluster-Knoten installieren.

Kaspersky Security Center Web Console auf den Knoten eines geografisch verteilten Failover-Clusters installieren

Für die Bereitstellung eines geografisch verteilten Kaspersky Security Center Linux-Failover-Clusters muss die Hochverfügbarkeit der Kaspersky Security Center Web Console gewährleistet sein. Um dies zu erreichen, muss die Kaspersky Security Center Web Console auf beiden Cluster-Knoten installiert werden.

So installieren Sie Kaspersky Security Center Web Console:

1. Legen Sie auf beiden Knoten einen einen Benutzer für die Arbeit mit Kaspersky Security Center Web Console an. Führen Sie dazu den folgenden Befehl unter einem Benutzerkonto mit Root-Rechten aus:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <password>
   ```

   Das Kennwort muss mindestens 8 Zeichen lang sein.

2. Lesen Sie auf beiden Knoten den Endbenutzer-Lizenzvertrag (EULA). Wenn das Programmpaket von Kaspersky Security Center Linux keine txt-Datei mit dem Text der EULA enthält, können Sie die Datei von der Kaspersky-Website herunterladen. Falls Sie den Lizenzvertrag ablehnen, installieren Sie die Anwendung nicht.

3. Erstellen Sie auf beiden Knoten eine Antwortdatei mit Parametern für die Verbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver: `/etc/ksc-web-console-setup.json`.

   Beispiel für eine Antwortdatei mit den minimal notwendigen Parametern

Die Gruppe an Parametern in der Antwortdatei hängt von der Version des Administrationsservers ab, mit welcher die Kaspersky Security Center Web Console verbunden ist:

- Administrationsserver ab Version 16

  Beispiel für eine Antwortdatei mit minimalen Parametern für die Anmeldung am Administrationsserver Version 16 oder höher:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Administrationsserver Version 15.4 oder niedriger

  Beispiel für eine Antwortdatei mit minimalen Parametern für die Anmeldung am Administrationsserver Version 15.4 oder niedriger:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Sie können die Kaspersky Security Center Web Console entweder auf demselben Gerät, auf dem der Administrationsserver installiert ist, oder auf einem anderen Gerät installieren. Wenn die Kaspersky Security Center Web Console auf einem anderen Gerät installiert ist, unterscheidet sich die Adresse der Kaspersky Security Center Web Console (durch `address` angegeben) von der Adresse des Administrationsservers (durch `iamHost` oder `kscHost` angegeben). Wenn die Kaspersky Security Center Web Console und der Administrationsserver auf demselben Gerät installiert sind, besitzen diese Parameter die gleichen Werte.

Der Wert `iamHost` muss mit der IAM-Adresse übereinstimmen, die Sie bei der Installation des Administrationsservers angegeben haben. Um die angegebene IAM-Adresse zu erhalten, führen Sie folgenden Befehl auf dem Gerät mit dem installierten Administrationsserver aus:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Weiter Informationen dazu finden Sie in folgendem Artikel: Installationsparameter für Kaspersky Security Center Web Console.

Sie können der Liste der vertrauenswürdigen Server mehrere Administrationsserver unterschiedlicher Versionen hinzufügen. In diesem Fall können die Server unterschiedliche Authentifizierungsmethoden verwenden.

Es wird empfohlen, Portnummern oberhalb von 1024 anzugeben. Wenn Sie möchten, dass Kaspersky Security Center Web Console auf den Ports unterhalb von 1024 funktioniert, stellen Sie nach der Installation sicher, dass Sie über das Tool "setcap" verfügen, und führen Sie den folgenden Befehl aus:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

Wenn Sie das setcap-Tool nicht besitzen, können Sie es installieren. **Klicken Sie auf diesen Link, um die Befehle anzuzeigen**.

Führen Sie für die Debian- und Ubuntu-Betriebssysteme einen der folgenden Befehle aus:

- `sudo apt-get install libcap2-bin`
- `sudo apt install libcap2-bin`

Führen Sie für SUSE Linux Enterprise Server und Red Hat Enterprise Linux den folgenden Befehl aus:

- `sudo zypper install libcap-progs`

4. Führen Sie auf beiden Knoten die Setup-Datei unter einem Benutzerkonto mit Root-Rechten aus.

```
sudo apt-get install ksc-web-console-<build number>.x86_64.deb
```

Dadurch wird die Installationsdatei entpackt. Bitte warten Sie, bis die Installation abgeschlossen ist. Kaspersky Security Center Web Console wird in den folgenden Pfad installiert: `/var/opt/kaspersky/ksc-web-console`.

5. Erstellen Sie auf einem der ClusterKnoten eine Pacemaker-Ressource für den Dienst "KSCWebConsole", um "KSCWebConsole" zu einem von Pacemaker verwalteten Dienst zu machen:

```
crm configure primitive ksc_webconsole systemd:KSCWebConsole \
op monitor interval=30s timeout=60s \
op start timeout=120s \
op stop timeout=120s \
meta target-role=Stopped
```

6. Stoppen Sie auf beiden Knoten den Dienst "KSCWebConsole" und deaktivieren Sie dessen Autostart:

```
sudo systemctl stop KSCWebConsole
sudo systemctl disable KSCWebConsole
```

7. Fügen Sie auf einem der Cluster-Knoten die Ressource `ksc_webconsole` der Gruppe `group_klfoc` hinzu:

```
crm configure edit klfoc_group
```

8. Fügen Sie am Ende der Gruppenzeile hinter `klfocsvc_dbms` den Wert `ksc_webconsole` hinzu, zum Beispiel:

```
group klfoc_group {
...
klfocsvc_dbms
ksc_webconsole
}
```

Nach dem erfolgreichen Abschluss der Installation können Sie in Ihrem Browser Kaspersky Security Center Web Console öffnen und sich einloggen.

Benutzerkonten für die Arbeit mit DBMS

Um den Administrationsserver zu installieren und zu verwenden, benötigen Sie ein internes DBMS-Konto. Dieses Konto ermöglicht Ihnen den Zugriff auf das DBMS und erfordert bestimmte Rechte. Die Zusammenstellung dieser erforderlichen Rechte hängt von folgenden Kriterien ab:

- DBMS-Typ:
  - MySQL oder MariaDB
  - PostgreSQL oder Postgres Pro
- Methode zur Erstellung der Administrationsserver-Datenbank:
  - **Automatisch**. Während der Installation des Administrationsservers können Sie automatisch eine Administrationsserver-Datenbank anlegen (auch als Serverdatenbank bezeichnet) indem Sie das Installationsprogramm des Administrationsservers (den Installer) verwenden.
  - **Manuell**. Sie können eine Drittanbieter-Anwendung oder ein Skript verwenden, um eine leere Datenbank zu erstellen. Anschließend können Sie die Datenbank während der Installation des Administrationsservers als Serverdatenbank angeben.

Befolgen Sie das Prinzip der geringsten Rechte, wenn Sie den Konten Rechte und Berechtigungen erteilen. Das bedeutet, dass die gewährte Rechte gerade ausreichend sein sollten, um die erforderlichen Aktionen auszuführen.

Nehmen Sie an der Datenbank des Administrationsservers und der IAM-Datenbank keine manuellen Änderungen vor. Dies schließt auch das Ändern von Werten und das Löschen oder Hinzufügen von Schemas, Tabellen oder Indizes mit ein. Jegliche Änderungen an den Datenbanken, die nicht vom Administrationsserver selbst vorgenommen werden, wirken sich früher oder später (z. B. nach einem Versions-Update oder nach der Wiederherstellung einer Backup-Kopie) auf die ordnungsgemäße Ausführung des Administrationsservers aus. Die direkte Bearbeitung von Datenbanken ist nur nach ausdrücklicher Anweisung des Technischen Supports von Kaspersky zulässig.

Die folgenden Tabellen enthalten Informationen über die DBMS-Rechte, die Sie den Konten gewähren sollten, bevor Sie den Administrationsserver installieren und starten.

MySQL und MariaDB

Wenn Sie MySQL oder MariaDB als DBMS auswählen, erstellen Sie ein internes DBMS-Konto für den Zugriff auf das DBMS und gewähren Sie diesem Konto anschließend die erforderlichen Rechte. Beachten Sie, dass die Art der Datenbankerstellung keinen Einfluss auf den Satz von Rechten hat. Die erforderlichen Rechte sind unten aufgeführt:

- Schema-Privilegien:
  - Administrationsserver-Datenbank: ALL (außer GRANT OPTION).
  - Systemschemata (mysql und sys): SELECT, SHOW VIEW.
  - Gespeicherte Prozedur sys.table_exists: EXECUTE (wenn Sie MariaDB 10.5 oder früher als DBMS verwenden,

müssen Sie das EXECUTE-Privileg nicht erteilen).

- Globale Privilegien für alle Schemata: PROCESS, SUPER.

Weitere Informationen zum Konfigurieren der Kontoberechtigungen finden Sie unter DBMS-Benutzerkonto für die Arbeit mit MySQL und MariaDB konfigurieren.

Ausführliche Informationen zum Verschieben von Daten aus einem gemeinsam genutzten Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich finden Sie unter Verschieben von Daten aus einem freigegebenen Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich in MySQL und MariaDB-DBMS.

Berechtigungen für die Wiederherstellung der Daten des Administrationsservers konfigurieren

Die Rechte, die Sie dem internen DBMS-Konto erteilt haben, reichen aus, um die Daten des Administrationsservers aus der Sicherung wiederherzustellen.

PostgreSQL oder Postgres Pro

Wenn Sie PostgreSQL oder Postgres Pro als DBMS auswählen, können Sie den Benutzer *Postgres* (die standardmäßige Postgres-Rolle) verwenden oder eine neue Postgres-Rolle (im Folgenden auch als Rolle bezeichnet) erstellen, um auf das DBMS zuzugreifen. Gewähren Sie der Rolle je nach Erstellungsmethode der Serverdatenbank die erforderlichen Rechte, wie in der folgenden Tabelle beschrieben. Weitere Informationen zum Konfigurieren der Rollenberechtigung finden Sie unter DBMS-Benutzerkonto für die Arbeit mit PostgreSQL oder Postgres Pro konfigurieren.

Rechte der Postgres-Rolle

Automatische Datenbankerstellung		Manuelle Datenbankerstellung
Der Benutzer *Postgres* benötigt keine weiteren Rechte.	Privilegien für eine neue Rolle: CREATEDB.	Für eine neue Rolle: • Privilegien für die Administrationsserver-Datenbank: ALL. • Privilegien für alle Tabellen im Schema "public": ALL. • Privilegien für alle Sequenzen im Schema "public": ALL.

Wenn eines hochverfügbaren Postgres-Clusters (Version 14 oder höher) als Datenbank verwendet wird, muss der Datenbankbenutzer über die Berechtigung `pg_read_all_stats` verfügen. Sie können diese Berechtigung erteilen, indem Sie den folgenden Befehl ausführen:

```
GRANT pg_read_all_stats TO "%1";
```

Wobei `%1` für den Namen des Datenbankbenutzers steht.

Der Benutzername wird während der Installation des Administrationsservers im Parameter `KLSRV_UNATT_DBMS_LOGIN` angegeben.

Berechtigungen für die Wiederherstellung der Daten des Administrationsservers konfigurieren

Um die Daten des Administrationsservers aus dem Backup wiederherzustellen, muss die Postgres-Rolle, die für den Zugriff auf das DBMS verwendet wird, über die Berechtigung "Owner" für die Administrationsserver-Datenbank verfügen.

DBMS-Benutzerkonto für die Arbeit mit MySQL und MariaDB konfigurieren

Erforderliche Vorrausetzungen

Bevor Sie dem DBMS-Benutzerkonto Rechte zuweisen, führen Sie die folgenden Maßnahmen aus:

1. Stellen Sie sicher, dass Sie unter dem lokalen Administratorkonto am System angemeldet sind.
2. Installieren Sie eine geeignete Umgebung für die Arbeit mit MySQL oder MariaDB.

Nehmen Sie an der Datenbank des Administrationsservers und der IAM-Datenbank keine manuellen Änderungen vor. Dies schließt auch das Ändern von Werten und das Löschen oder Hinzufügen von Schemas, Tabellen oder Indizes mit ein. Jegliche Änderungen an den Datenbanken, die nicht vom Administrationsserver selbst vorgenommen werden, wirken sich früher oder später (z. B. nach einem Versions-Update oder nach der Wiederherstellung einer Backup-Kopie) auf die ordnungsgemäße Ausführung des Administrationsservers aus. Die direkte Bearbeitung von Datenbanken ist nur nach ausdrücklicher Anweisung des Technischen Supports von Kaspersky zulässig.

Konfigurieren des DBMS-Benutzerkontos, um den Administrationsserver zu installieren

So konfigurieren Sie das DBMS-Benutzerkonto für die Installation des Administrationsservers:

1. Führen Sie eine Umgebung zum Arbeiten mit MySQL oder MariaDB unter dem Root-Konto aus, das Sie bei der Installation des DBMS erstellt haben.
2. Erstellen Sie ein internes DBMS-Konto mit einem Passwort. Das Installationsprogramm des Administrationsservers (im Folgenden auch als Installer bezeichnet) und der Dienst des Administrationsservers des Administrationsservers verwenden dieses interne DBMS-Konto für den Zugriff auf das DBMS.

   Um ein DBMS-Konto mit einem Kennwort zu erstellen, führen Sie den folgenden Befehl aus:

   ```
   /* Benutzer namens kscdbadmin erstellen und Kennwort für kscdbadmin angeben*/
   CREATE USER 'kscdbadmin' IDENTIFIED BY '<Kebnnwort>';
   ```

3. Gewähren Sie dem erstellten DBMS-Konto die folgenden Privilegien:

   - Schema-Privilegien:
     - Administrationsserver-Datenbank: ALL (außer GRANT OPTION)
     - Systemschemata (mysql und sys): SELECT, SHOW VIEW
     - Die gespeicherte Prozedur sys.table_exists: EXECUTE
   - Globale Privilegien für alle Schemata: PROCESS, SUPER

   Führen Sie das folgende Skript aus, um dem erstellten DBMS-Konto die erforderlichen Berechtigungen zu erteilen:

   ```
   /* kscdbadmin Berechtigungen gewähren */
   ```

```
GRANT USAGE ON *.* TO 'kscdbadmin';
GRANT ALL ON kav.* TO 'kscdbadmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'kscdbadmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'kscdbadmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin';
GRANT PROCESS ON *.* TO 'kscdbadmin';
GRANT SUPER ON *.* TO 'kscdbadmin';
```

Wenn Sie MariaDB 10.5 oder früher als DBMS verwenden, müssen Sie das EXECUTE-Privileg nicht erteilen. Schließen Sie in diesem Fall den folgenden Befehl aus dem Skript aus: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'kscdbadmin'`.

4. Führen Sie den folgenden Befehl aus, um die Liste der Berechtigungen anzuzeigen, die dem DBMS-Konto gewährt wurden:

   ```
   SHOW grants for 'kscdbadmin';
   ```

5. Erstellen Sie für IAM ein DBMS-Konto. Führen Sie den folgenden Befehl aus:

   ```
   /* Benutzer namens `iamdbadmin` anlegen und Kennwort für `iamdbadmin` erstellen */
   CREATE USER 'iamdbadmin' IDENTIFIED BY '<password>';
   ```

   Wenn Sie MySQL 8.0 oder früher als DBMS verwenden, beachten Sie, dass für diese Versionen die "Caching SHA2 password"-Authentifizierung nicht unterstützt wird. Ändern Sie die Standardauthentifizierung von "Caching SHA2 password" in "MySQL native password":

   - Führen Sie den folgenden Befehl aus, um ein DBMS-Konto zu erstellen, das die "MySQL native password"-Authentifizierung verwendet:

     ```
     CREATE USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '<Kennwort>';
     ```

   - Führen Sie den folgenden Befehl aus, um die Authentifizierung für ein vorhandenes DBMS-Konto zu ändern:

     ```
     ALTER USER 'iamdbadmin'@'%' IDENTIFIED WITH mysql_native_password BY '<Kennwort>';
     ```

6. Gewähren Sie dem erstellten DBMS-Konto die folgenden Privilegien:

   - Schema-Privilegien:
     - Administrationsserver-Datenbank: ALL (außer GRANT OPTION)
     - Systemschemata (mysql und sys): SELECT, SHOW VIEW
     - Die gespeicherte Prozedur sys.table_exists: EXECUTE
   - Globale Privilegien für alle Schemata: PROCESS, SUPER

   Führen Sie das folgende Skript aus, um dem erstellten DBMS-Konto die erforderlichen Berechtigungen zu erteilen:

   ```
   /* `iamdbadmin` Berechtigungen gewähren */
   GRANT USAGE ON *.* TO 'iamdbadmin';
   GRANT ALL ON iamdb.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'iamdbadmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'iamdbadmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin';
   ```

```
GRANT PROCESS ON *.* TO 'iamdbadmin';
GRANT SUPER ON *.* TO 'iamdbadmin';
```

Wenn Sie MariaDB 10.5 oder früher als DBMS verwenden, müssen Sie das EXECUTE-Privileg nicht erteilen. Schließen Sie in diesem Fall den folgenden Befehl aus dem Skript aus: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'iamdbadmin'`.

7. Führen Sie den folgenden Befehl aus, um die Liste der Berechtigungen anzuzeigen, die dem DBMS-Konto gewährt wurden:

   ```
   SHOW grants for 'iamdbadmin';
   ```

8. Um eine Administrationsserver-Datenbank manuell zu erstellen, führen Sie den folgenden Befehl aus (in diesem Befehl lautet der Name der Administrationsserver-Datenbank *kav*):

   ```
   CREATE DATABASE kav
   ```

   Verwenden Sie denselben Datenbanknamen, den Sie in dem Skript angeben, welches das DBMS-Konto erstellt.

9. Um eine IAM-Datenbank manuell anzulegen, führen Sie das folgende Skript aus (in diesem Befehl lautet der Name der IAM-Datenbank *iam*):

   ```
   CREATE DATABASE iam
   ```

   Der Administrationsserver löscht die IAM-Datenbank nicht automatisch, wenn der Server deinstalliert oder auf ein anderes Gerät verschoben wird. Sie müssen die Datenbank manuell entfernen.

10. Installieren Sie den Administrationsserver.

Nach Abschluss der Installation wird die Administrationsserver-Datenbank erstellt und der Administrationsserver ist einsatzbereit.

DBMS-Benutzerkonto für die Arbeit mit PostgreSQL und Postgres Pro konfigurieren

Erforderliche Vorrausetzungen

Bevor Sie dem DBMS-Benutzerkonto Rechte zuweisen, führen Sie die folgenden Maßnahmen aus:

1. Stellen Sie sicher, dass Sie unter dem lokalen Administratorkonto am System angemeldet sind.
2. Installieren Sie eine geeignete Umgebung für die Arbeit mit PostgreSQL und Postgres Pro.
3. PostgreSQL- oder Postgres Pro-Server für die Ausführung mit Kaspersky Security Center Linux konfigurieren.

Nehmen Sie an der Datenbank des Administrationsservers und der IAM-Datenbank keine manuellen Änderungen vor. Dies schließt auch das Ändern von Werten und das Löschen oder Hinzufügen von Schemas, Tabellen oder Indizes mit ein. Jegliche Änderungen an den Datenbanken, die nicht vom Administrationsserver selbst vorgenommen werden, wirken sich früher oder später (z. B. nach einem Versions-Update oder nach der Wiederherstellung einer Backup-Kopie) auf die ordnungsgemäße Ausführung des Administrationsservers aus. Die direkte Bearbeitung von Datenbanken ist nur nach ausdrücklicher Anweisung des Technischen Supports von Kaspersky zulässig.

Konfigurieren Sie die DBMS-Benutzerkonten, um den Administrationsserver zu installieren

So konfigurieren Sie die DBMS-Benutzerkonten für die Installation des Administrationsservers:

1. Starten Sie eine Umgebung für die Arbeit mit Postgres.
2. Melden Sie sich als Benutzer *Postgres* an der *Postgres*-Datenbank an.
3. Erstellen Sie eine neue Postgres-Rolle (in diesem Beispiel heißt die Rolle *kscdbadmin*):

   ```
   CREATE USER "kscdbadmin" WITH PASSWORD '<password>';
   ```

4. Erstellen Sie eine Datenbank für den Administrationsserver (in diesem Beispiel ist der Name dieser Datenbank `kav`):

   ```
   CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";
   ```

   Es wird empfohlen, die Postgres-Rolle anzugeben, die Sie in Schritt 3 dieser Anleitung als Datenbankbesitzer angegeben haben (in diesem Beispiel ist die Rolle *kscdbadmin*).

   Anderen Benutzer als Datenbankeigentümer angeben

   Wenn Sie eine andere Postgres-Rolle angeben möchten, verbinden Sie sich mit der Datenbank unter dieser Benutzerrolle (oder als "superuser") und führen Sie die folgenden Befehle aus:

   ```
   GRANT ALL PRIVILEGES ON DATABASE "kav" TO "kscdbadmin";
   GRANT USAGE ON SCHEMA public TO "kscdbadmin";
   GRANT CREATE ON SCHEMA public TO "kscdbadmin";
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "kscdbadmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "kscdbadmin";
   ```

   Stellen Sie sicher, dass die Rolle des Datenbankbesitzers die Privilegien CONNECT und TEMPORARY besitzt.

   Wenn die Fehlermeldung "New encoding (UTF8) is incompatible with the encoding of the template database" erscheint, erstellen Sie eine Datenbank mit dem Befehl:
   `CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin" TEMPLATE template0;`
   anstelle von:
   `CREATE DATABASE "kav" ENCODING 'UTF8' OWNER "kscdbadmin";`

5. Erstellen Sie eine neue Postgres-Rolle für IAM (in diesem Beispiel heißt die Postgres-Rolle `iamdbadmin`):

   ```
   CREATE USER "iamdbadmin" WITH PASSWORD '<password>';
   ```

6. Erstellen Sie eine IAM-Datenbank (in diesem Beispiel , lautet der Name der IAM-Datenbank `iam`):

   ```
   CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";
   ```

   Es wird empfohlen, die Postgres-Rolle anzugeben, die Sie in Schritt 3 dieser Anleitung als Datenbankbesitzer angegeben haben (in diesem Beispiel ist die Rolle *iamdbadmin*).

   Anderen Benutzer als IAM-Datenbankeigentümer angeben

Wenn Sie eine andere Postgres-Rolle angeben möchten, verbinden Sie sich mit der Datenbank unter dieser Benutzerrolle (oder als "superuser") und führen Sie die folgenden Befehle aus:

```
GRANT ALL PRIVILEGES ON DATABASE "iam" TO "iamdbadmin";
GRANT USAGE ON SCHEMA public TO "iamdbadmin";
GRANT CREATE ON SCHEMA public TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "iamdbadmin";
GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "iamdbadmin";
```

Stellen Sie sicher, dass die Rolle des Datenbankbesitzers die Privilegien CONNECT und TEMPORARY besitzt.

> Wenn die Fehlermeldung "New encoding (UTF8) is incompatible with the encoding of the template database" erscheint, erstellen Sie eine Datenbank mit dem Befehl:
> `CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin" TEMPLATE template0;`
> anstelle von:
> `CREATE DATABASE "iam" ENCODING 'UTF8' OWNER "iamdbadmin";`

Der Administrationsserver löscht die IAM-Datenbank nicht automatisch, wenn der Server deinstalliert oder auf ein anderes Gerät verschoben wird. Sie müssen die Datenbank manuell entfernen.

7. Installieren Sie den Administrationsserver.

Nach Abschluss der Installation verwendet der Administrationsserver die erstellte Datenbank zum Speichern der Daten des Administrationsservers. Der Administrationsserver ist einsatzbereit.

In MySQL und MariaDB-DBMS Daten aus einem freigegebenen Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich verschieben

Für ein MySQL- und MariaDB-DBMS können Sie Daten auf folgende Weise speichern:

- Als gemeinsam genutzter Tabellenbereich, wenn die Daten aller Benutzer-Datenbanken in einer einzigen Datei gespeichert sind (normalerweise in der Datei `ibdata1`).
- Als Tabellenbereich für Dateien pro Tabelle, wenn für jede Tabelle ein separater Datenbereich als separate Datei erstellt wird.

Die Verwendung eines gemeinsam genutzten Tabellenbereichs erhöht das Risiko der Fragmentierung des Tabellenbereichs. Da es nicht möglich ist, eine `SHRINK`-Operation auszuführen, kann eine Datei in einem gemeinsam genutzten Tabellenbereich etwa 90 % des Speicherplatzes einnehmen. Dies wirkt sich negativ auf die Leistung des Datenträgersubsystems aus. Daher ist es sinnvoll, sich für einen Tabellenbereich für Dateien pro Tabelle zu entscheiden.

In diesem Artikel wird beschrieben, wie Sie Daten aus einem gemeinsam genutzten Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich verschieben. Wenn das MySQL- oder MariaDB-DBMS auch von anderen Anwendungen verwendet wird, müssen Sie die Datenbanken dieser Anwendungen in den Datei-pro-Tabelle-Tabellenbereich verschieben.

> Es wird empfohlen, dieses Verfahren nur auszuführen, wenn Sie ein MySQL- oder MariaDB-DBMS für den Administrationsserver verwenden.
> Das Verschieben von Daten aus einem gemeinsam genutzten Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich kann die Belastung des Festplatten-Subsystems erhöhen.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie Folgendes sicher:

- Sie haben eine Backup-Kopie der Daten des Administrationsservers erstellt, indem Sie entweder eine Aufgabe zur Datensicherung oder das Dienstprogramm klbackup ausgeführt haben.
- Sie haben eine Backup-Kopie anderer Anwendungen erstellt, deren Anwendungsdatenbanken von einem MySQL- oder MariaDB-DBMS (falls vorhanden) verwaltet werden.
- Auf dem Gerät, auf dem das DBMS installiert ist, ist in der Partition mit der Datenbank freier Speicherplatz auf der Festplatte vorhanden.

Der erforderliche Speicherplatz beträgt 150 % der aktuellen Gesamtgröße der Datenbanken (aktuelle Größe der Datei `ibdata1`).

Prozess

Gehen Sie wie folgt vor, um Daten aus einem gemeinsam genutzten Tabellenbereich in einen Tabellenbereich für Dateien pro Tabelle zu verschieben:

1. Stoppen Sie den Kaspersky Security Center Administrationsserver und andere Anwendungen, welche die gleiche DBMS-Instanz verwenden, für die Sie diesen Vorgang ausführen möchten.
2. Melden Sie sich je nach DBMS-Version als Superuser an Ihrem DBMS an und führen Sie anschließend in einer beliebigen Anwendung das Skript `fix_tablespace.sql` aus.

   Sie können die Skripte `fix_tablespace.sql` anzeigen, indem Sie auf diese Links klicken:

   Das Skript für MySQL 5.7 und MariaDB 10.1+ anzeigen

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

   Das Skript für MySQL 8.0+ anzeigen

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
```

```
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;
    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';' );
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;
        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Sie dürfen die Skriptausführung nicht stoppen.
Wenn keine DBMS-Fehler aufgetreten sind, Sie aber die Skriptausführung beendet haben, führen Sie entweder das Skript erneut durch oder stoppen Sie die Schritte dieses Verfahrens, starten Sie den DBMS-Dienst neu und stellen Sie die Daten des Administrationsservers aus der Sicherung wieder her.

3. Setzen Sie im Abschnitt `[mysqld]` der Datei my.cnf den Parameter `innodb_file_per_table` auf `1`.
4. Starten Sie den MySQL oder MariaDB-Dienst neu.
5. Starten Sie den Dienst des Kaspersky Security Center Administrationsservers neu.

Die Daten werden von einem gemeinsam genutzten Tabellenbereich in einen Datei-pro-Tabelle-Tabellenbereich verschoben.

Zertifikate für die Ausführung mit Kaspersky Security Center Linux

Dieser Abschnitt enthält Informationen über die Zertifikate für Kaspersky Security Center Linux. Außerdem wird hier beschrieben, wie Sie Zertifikate für Kaspersky Security Center Web Console ausstellen und ersetzen und wie Sie ein Zertifikat für den Administrationsserver erneuern, wenn der Server mit Kaspersky Security Center Web Console interagiert.

Über die Zertifikate von Kaspersky Security Center

Um eine sichere Interaktion zwischen den Komponenten der Anwendung zu ermöglichen, verwendet Kaspersky Security Center die folgenden Arten von Zertifikaten:

- Zertifikat des Administrationsservers
- Mobilgerät-Zertifikat
- Zertifikat des Webservers
- Zertifikat der Kaspersky Security Center Web Console
- Zertifikat der Identitäts- und Zugriffsverwaltung

Standardmäßig verwendet Kaspersky Security Center selbstsignierte Zertifikate (d.h., sie werden von Kaspersky Security Center selbst ausgestellt). Sie können diese jedoch durch benutzerdefinierte Zertifikate ersetzen, um den Sicherheitsanforderungen Ihres Unternehmensnetzwerks sowie Sicherheitsstandards besser zu entsprechen. Wenn Sie ein benutzerdefiniertes Zertifikat verwenden, muss die Zertifikatsdatei die vollständige Kette der öffentlichen Schlüssel enthalten, einschließlich aller Zwischenzertifikate bis hin zur Stammzertifizierungsstelle (CA). Nachdem der Administrationsserver sichergestellt hat, dass das benutzerdefinierte Zertifikat alle notwendigen Anforderungen erfüllt, nimmt das Zertifikat den gleichen Funktionsumfang wie ein selbstsigniertes Zertifikat an. Der einzige Unterschied besteht darin, dass ein benutzerdefiniertes Zertifikat nach dessen Ablauf nicht automatisch neu ausgestellt wird. Zertifikate können durch benutzerdefinierte Zertifikate ersetzt werden, indem Sie entweder das Dienstprogramm klsetsrvcert verwenden oder je nach Zertifikattyp den Abschnitt "Eigenschaften des Administrationsservers" in Kaspersky Security Center Web Console verwenden. Wenn Sie das Tool "klsetsrvcert" verwenden, müssen Sie für das Zertifikat einen Typ angeben, indem Sie einen der folgenden Werte verwenden:

- C – gewöhnliches Zertifikat für die Ports 13000 und 13291
- CR – gewöhnliches Reservezertifikat für die Ports 13000 und 13291
- M – Mobilgerät-Zertifikat für den Port 13292
- MR – mobiles Reservezertifikat für den Port 13292
- MCA – mobile Zertifizierungsstelle für automatisch generierte Benutzerzertifikate

Die maximale Gültigkeitsdauer für jedes Zertifikat des Administrationsservers beträgt 397 Tage.

Zertifikate des Administrationsservers

Ein Zertifikat des Administrationsservers ist für folgende Zwecke erforderlich:

- Authentifizierung des Administrationsservers, wenn sich Kaspersky Security Center Web Console mit ihm verbindet.
- Sichere Interaktion zwischen dem Administrationsserver und dem Administrationsagenten auf verwalteten Geräten.
- Authentifizierung, wenn die primären Administrationsserver mit sekundären Administrationsservern verbunden sind.

Das Zertifikat des Administrationsservers wird bei der Installation der Komponente "Administrationsserver" automatisch erstellt und im Ordner /var/opt/kaspersky/klnagent_srv/1093/cert/ gespeichert. Das Zertifikat des Administrationsservers geben Sie an, wenn Sie eine Antwortdatei erstellen, um Kaspersky Security Center Web Console zu installieren. Dieses Zertifikat wird als gewöhnliches Zertifikat (common - "C") bezeichnet.

Das Zertifikat des Administrationsservers ist für 397 Tage gültig. Kaspersky Security Center generiert CR-Zertifikat ("common reserve") automatisch 90 Tage vor Ablauf des gewöhnlichen Zertifikats. Das gewöhnliche Reservezertifikat wird daraufhin für das nahtlose Ersetzen des Zertifikats des Administrationsservers verwendet. Wenn das gemeinsame Zertifikat im Begriff ist abzulaufen, wird das gemeinsame Reservezertifikat verwendet, um die Verbindung mit den Instanzen der Administrationsagenten auf den verwalteten Geräten aufrecht zu erhalten. Aus diesem Grund wird 24 Stunden vor Ablauf des alten gewöhnlichen Zertifikates das gewöhnliche Reservezertifikat automatisch zum neuen gewöhnlichen Zertifikat.

Die maximale Gültigkeitsdauer für jedes Zertifikat des Administrationsservers beträgt 397 Tage.

Bei Bedarf können Sie dem Administrationsserver ein benutzerdefiniertes Zertifikat zuweisen. Dies kann beispielsweise für eine bessere Integration in die vorhandene PKI Ihres Unternehmens oder für die benutzerdefinierte Konfiguration der Zertifikatfelder erforderlich sein. Beim Ersetzen des Zertifikates stellen alle Administrationsagenten, die zuvor mittels SSL mit Administrationsserver verbunden waren, keine Verbindung mit dem Server mehr her und geben den Fehler "Fehler bei der Authentifizierung des Administrationsservers" zurück. Um diesen Fehler zu beheben, müssen Sie die Verbindung nach dem Ersetzen des Zertifikats wiederherstellen.

Nachdem das Zertifikat des Administrationsservers durch ein Reserve-Zertifikat oder benutzerdefiniertes Zertifikat ersetzt wurde, geben Sie das neue Zertifikat in der Antwortdatei an und installieren Sie Kaspersky Security Center Web Console mithilfe dieser Datei erneut. Andernfalls kann die Kaspersky Security Center Web Console keine Verbindung zum Administrationsserver herstellen.

Sollte das Zertifikat des Administrationsservers verloren gehen, sind zu dessen Wiederherstellung eine Neuinstallation der Komponente "Administrationsserver" und eine anschließende Wiederherstellung der Daten erforderlich.

Außerdem können Sie für das Zertifikat des Administrationsservers eine Sicherungskopie, die von anderen Einstellungen des Administrationsservers separiert ist, erstellen, um so den Administrationsserver ohne Datenverlust von einem Gerät auf ein anderes verlegen zu können.

Wenn Sie Kaspersky Security Center Web Console in verschiedenen Browsern öffnen und im Eigenschaftenfenster des Administrationsservers die Datei mit dem Zertifikat des Administrationsservers herunterladen, haben die Dateien unterschiedliche Namen.

Mobilgerät-Zertifikate

Ein Mobilgerät-Zertifikat (mobile - "M") wird für die Authentifizierung des Administrationsservers auf mobilen Geräten verwendet. Das Mobilgerät-Zertifikat geben Sie in den Eigenschaften des Administrationsservers an.

Es existiert außerdem ein Mobilgerät-Reservezertifikat ("MR"): Dieses wird für das nahtlose Ersetzen des Mobilgerät-Zertifikats verwendet. Kaspersky Security Center generiert dieses Zertifikat 60 Tage vor Ablauf des gemeinsamen Zertifikats automatisch. Wenn das Mobilgerät-Zertifikat dabei ist abzulaufen, wird das Mobilgerät-Reservezertifikat verwendet, um die Verbindung mit den Instanzen der Administrationsagenten auf den verwalteten mobilen Geräten aufrecht zu erhalten. Aus diesem Grund wird 24 Stunden vor Ablauf des alten Mobilgerät-Zertifikats das Mobilgerät-Reservezertifikat automatisch zum neuen mobilen Zertifikat.

Wenn Sie für Ihr Verbindungsszenario Client-Zertifikate auf den mobilen Geräten benötigen (für Verbindungen unter Verwendung von Two-Way SSL), können Sie diese Zertifikate unter Verwendung der Zertifizierungsstelle für automatisch generierte Benutzerzertifikate (Mobile Certificate Authority -"MCA") erstellen. Außerdem können Sie in den Eigenschaften des Administrationsservers benutzerdefinierte Zertifikate angeben, die von einer anderen Zertifizierungsstelle ausgestellt wurden, während die Integration mit der Domain Public Key Infrastructure (PKI) Ihrer Organisation es Ihnen ermöglicht, Client-Zertifikate durch Ihre Domain-Zertifizierungsstelle auszustellen.

Um den Administrationsservers auf mobilen Geräten mit iOS-Betriebssystem authentifizieren zu können, ist zusätzlich ein iOS MDM-Server-Zertifikat erforderlich. Weitere Informationen finden Sie unter Zertifikat für den iOS MDM-Server konfigurieren

https://support.kaspersky.com/help/KSMM/5.0/en-US/287007.htm
.

Zertifikat des Webservers

Die Webserver-Komponente des Kaspersky Security Center Administrationsservers verwendet einen speziellen Zertifikatstyp. Dieses Zertifikat wird für die Veröffentlichung von Installationspaketen für den Administrationsagenten, die Sie anschließend auf Ihre verwalteten Geräte herunterladen, sowie für Kaspersky Security for Mobil benötigt. Aus diesem Grund kann der Webserver verschiedene Zertifikate verwenden.

Wenn die Unterstützung von mobilen Geräten deaktiviert ist, verwendet der Webserver eins der folgenden Zertifikate, gegliedert nach Priorität:

1. Benutzerdefiniertes Zertifikat des Webservers, welches Sie manuell in der Verwaltungskonsole angegeben haben
2. Gewöhnliches Zertifikate des Administrationsservers ("C")

Wenn die Unterstützung von mobilen Geräten aktiviert ist, verwendet der Webserver eins der folgenden Zertifikate, gegliedert nach Priorität:

1. Benutzerdefiniertes Zertifikat des Webservers, welches Sie manuell in der Verwaltungskonsole angegeben haben
2. Benutzerdefiniertes Mobilgerät-Zertifikat
3. Selbstsigniertes Mobilgerät-Zertifikat ("M")
4. Gewöhnliches Zertifikate des Administrationsservers ("C")

Zertifikat der Kaspersky Security Center Web Console

Der Server der Web Console von Kaspersky Security Center (im Folgenden als Web Console bezeichnet) verfügt über ein eigenes Zertifikat. Wenn Sie eine Website öffnen, überprüft ein Browser, ob Ihre Verbindung vertrauenswürdig ist. Das Zertifikat der Web Console ermöglicht Ihnen die Authentifizierung der Web Console und wird verwendet, um den Datenverkehr zwischen einem Browser und der Web Console zu verschlüsseln.

Wenn Sie die Web Console öffnen, informiert Sie der Browser möglicherweise darüber, dass die Verbindung zur Web Console nicht privat und das Zertifikat der Web Console ungültig ist. Diese Warnung wird angezeigt, weil das Zertifikat der Web Console selbstsigniert ist und von Kaspersky Security Center automatisch generiert wird. Um diese Warnung zu vermeiden, können Sie Folgendes tun:

- Ersetzen Sie das Zertifikat der Web Console mit einem benutzerdefinierten (empfohlene Option). Erstellen Sie ein Zertifikat, das in Ihrer Infrastruktur vertrauenswürdig ist und das die Anforderungen an benutzerdefinierte Zertifikate erfüllt.
- Fügen Sie das Zertifikat der Web Console zur Liste der vertrauenswürdigen Zertifikate des Browsers hinzu. Es wird empfohlen, dass Sie diese Option nur verwenden, wenn Sie kein benutzerdefiniertes Zertifikat erstellen können.

Zertifikat der Identitäts- und Zugriffsverwaltung

Ein Zertifikat für die Identitäts- und Zugriffsverwaltung (IAM-Zertifikat) wird für die folgenden Zwecke benötigt:

- Authentifizierung des Administrationsservers, wenn sich der Browser eines Benutzers über das OAuth-Protokoll mit ihm verbindet.
- Authentifizierung des Administrationsservers, wenn sich Kaspersky Security Center Web Console mit ihm verbindet.

Das IAM-Zertifikat wird beim ersten Start des Administrationsservers automatisch erstellt. Das Zertifikat wird auf dem Gerät des Administrationsservers in folgendem Verzeichnis gespeichert: /var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem (für ein Failover-Cluster von Kaspersky Security Center: <shared data folder>/iam/main_certificate.pem). Wenn Sie eine Antwortdatei für die Installation von Kaspersky Security Center Web Console erstellen, müssen Sie den Pfad des IAM-Zertifikats mithilfe des Parameters `iamCertPath` angeben.

Das IAM-Zertifikat ist für 365 Tage gültig. Kaspersky Security Center generiert 48 Stunden vor Ablauf des aktuellen Zertifikats automatisch ein Reserve-Zertifikat. Das Reservezertifikat wird anschließend für das nahtlose Ersetzen des abgelaufenen IAM-Zertifikats verwendet.

Die maximale Gültigkeitsdauer für jedes IAM-Zertifikat beträgt 397 Tage.

Bei Bedarf können Sie ein benutzerdefiniertes IAM-Zertifikat zuweisen. Dies kann beispielsweise für eine bessere Integration in die vorhandene PKI Ihres Unternehmens oder für die benutzerdefinierte Konfiguration der Zertifikatfelder erforderlich sein.

> Nachdem das IAM-Zertifikat durch ein Reserve-Zertifikat oder benutzerdefiniertes Zertifikat ersetzt wurde, geben Sie das neue Zertifikat in der Antwortdatei an und installieren Sie Kaspersky Security Center Web Console mithilfe dieser Datei erneut. Andernfalls kann die Kaspersky Security Center Web Console keine Verbindung zum Administrationsserver herstellen.

Wenn Sie sich an der Kaspersky Security Center Web Console anmelden, wird der Browser zur Anmeldeseite des Administrationsservers (https://`<Administrationsserver-Adresse>`:4444) zur Authentifizierung weitergeleitet. Der Datenverkehr zwischen dem Browser und dem Administrationsserver wird mithilfe des TLS-Protokolls und des IAM-Zertifikats verschlüsselt.

Der Browser informiert Sie möglicherweise darüber, dass die Verbindung zum Administrationsserver nicht privat und dass das IAM-Zertifikat ungültig ist. Diese Warnung wird angezeigt, weil das IAM-Zertifikat selbst signiert ist und von Kaspersky Security Center automatisch generiert wird. Um diese Warnung zu vermeiden, können Sie Folgendes tun:

- Ersetzen Sie das IAM-Zertifikat durch ein benutzerdefiniertes Zertifikat (empfohlene Option). Erstellen Sie ein Zertifikat, das in Ihrer Infrastruktur vertrauenswürdig ist und das die Anforderungen an benutzerdefinierte Zertifikate erfüllt.

- Fügen Sie das IAM-Zertifikat zur Liste der vertrauenswürdigen Zertifikate des Browsers hinzu. Es wird empfohlen, dass Sie diese Option nur verwenden, wenn Sie kein benutzerdefiniertes Zertifikat erstellen können.

Anforderungen an benutzerdefinierte Zertifikate für deren Verwendung in Kaspersky Security Center Linux

Die unten stehende Tabelle zeigt die Voraussetzungen für benutzerdefinierte Zertifikate, angegeben in Bezug auf verschiedene Komponenten von Kaspersky Security Center Linux, an.

Voraussetzungen für Zertifikate von Kaspersky Security Center Linux

Typ des Zertifikats	Voraussetzungen	Kommentare
Gewöhnliches Zertifikat, gewöhnliches Reservezertifikat ("C", "CR")	Minimale Schlüssellänge: 2048 Basic constraints: • Path Length Constraint: None Schlüsselverwendung: • Digital signature • Certificate signing • Key encipherment • CRL Signing Extended Key Usage (optional): Serverauthentifizierung, Clientauthentifizierung Das Zertifikat muss einen gültigen "Subject Alternative Name" (SAN) enthalten, der die Loopback-Adresse des Administrationsservers enthält: • Für IPv4: 127.0.0.1 • Für IPv6: 0:0:0:0:0:0:0:1	Der Parameter für Extended Key Usage ist optional. Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, aber darf nicht kleiner als "1" sein.
Zertifikat des Webservers	Extended Key Usage: Serverauthentifizierung Der PKCS #12- / PEM-Container, aus dem das Zertifikat angegeben wird, enthält die vollständige Kette der öffentlichen Schlüssel. Der "Subject Alternative Name" (SAN) des Zertifikats ist vorhanden. Das heißt, dass der Wert des Feldes `subjectAltName` zulässig ist. Das Zertifikat erfüllt die aktuell wirksamen Anforderungen des Webbrowsers an Serverzertifikate, sowie die aktuell gültigen Grundvoraussetzungen des CA/Browser Forums.	–
Zertifikat der Kaspersky Security Center Web Console	Extended Key Usage: Serverauthentifizierung, Clientauthentifizierung Der PEM-Container, aus dem das Zertifikat angegeben wird, enthält die vollständige Kette der öffentlichen Schlüssel. Der "Subject Alternative Name" (SAN) des Zertifikats ist vorhanden. Das heißt, dass der Wert des Feldes `subjectAltName` zulässig ist. Der Wert muss mit der IAM-Adresse übereinstimmen, die bei der Installation des Administrationsservers angegeben wurde. Um die angegebene IAM-Adresse zu erhalten, führen Sie folgenden Befehl auf dem Host des Administrationsservers aus: `grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` Das Zertifikat erfüllt die aktuell wirksamen Anforderungen des Webbrowsers an Serverzertifikate, sowie die aktuell gültigen Grundvoraussetzungen des CA/Browser Forums.	Verschlüsselte Zertifikate werden von Kaspersky Security Center Web Console nicht unterstützt.

Typ des Zertifikats	Voraussetzungen	Kommentare
Zertifikat der Identitäts- und Zugriffsverwaltung (IAM-Zertifikat)	Extended Key Usage: Serverauthentifizierung Der PEM-Container, aus dem das Zertifikat angegeben wird, enthält die vollständige Kette der öffentlichen Schlüssel. Das Zertifikat muss gültig sein und die Client-Authentifizierung unterstützen. Das Zertifikat erfüllt die aktuell wirksamen Anforderungen des Webbrowsers an Serverzertifikate, sowie die aktuell gültigen Grundvoraussetzungen des CA/Browser Forums.	Verschlüsselte Zertifikate werden von Kaspersky Security Center Web Console nicht unterstützt.

Zertifikat für Kaspersky Security Center Web Console erneut ausstellen

In den meisten Browser gilt eine maximale Gültigkeitsdauer für Zertifikate. Um diese Bedingung einzuhalten, ist die Gültigkeitsdauer des Zertifikats für Kaspersky Security Center Web Console auf 397 Tage begrenzt. Sie können ein vorhandenes Zertifikat ersetzen, das von einer Zertifizierungsstelle (Certification Authority, CA) stammt. Dazu stellen Sie ein neues, selbstsigniertes Zertifikat aus. Alternativ können Sie Ihr abgelaufenes Zertifikat von Kaspersky Security Center Web Console neu ausstellen.

Das Zertifikat für Kaspersky Security Center Web Console kann nicht automatisch neu ausgestellt werden. Sie müssen das abgelaufene Zertifikat manuell neu ausstellen.

Wenn Sie Kaspersky Security Center Web Console öffnen, informiert der Browser möglicherweise darüber, dass die Verbindung zu Kaspersky Security Center Web Console nicht geschützt ist und dass das Zertifikat der Kaspersky Security Center Web Console ungültig ist. Diese Warnung wird angezeigt, weil das Zertifikat der Web Console selbstsigniert ist und von Kaspersky Security Center Linux automatisch generiert wird. Um diese Warnung zu entfernen oder zu vermeiden, können Sie Folgendes tun:

- Geben Sie bei der Neuausstellung des Zertifikats ein benutzerdefiniertes Zertifikat an (empfohlene Option). Erstellen Sie ein Zertifikat, das in Ihrer Infrastruktur vertrauenswürdig ist und das die Anforderungen an benutzerdefinierte Zertifikate erfüllt.

- Fügen Sie das Zertifikat für Kaspersky Security Center Web Console nach der Neuausstellung zur Liste der vertrauenswürdigen Browser-Zertifikate hinzu. Es wird empfohlen, dass Sie diese Option nur verwenden, wenn Sie kein benutzerdefiniertes Zertifikat erstellen können.

So stellen Sie ein abgelaufenes Zertifikat von Kaspersky Security Center Web Console neu aus:

Installieren Sie Kaspersky Security Center Web Console neu. Dafür gibt es die folgenden Methoden:

- Wenn Sie dieselbe Installationsdatei für Kaspersky Security Center Web Console verwenden möchten, entfernen Sie Kaspersky Security Center Web Console und installieren Sie anschließend die gleiche Version von Kaspersky Security Center Web Console.

- Wenn Sie die Installationsdatei einer aktualisierten Version verwenden möchten, führen Sie den Upgrade-Befehl aus.

Das Zertifikat von Kaspersky Security Center Web Console wurde erneut für eine weitere Gültigkeitsdauer von 397 Tagen ausgestellt.

Zertifikat für Kaspersky Security Center Web Console ersetzen

Wenn Sie den Server der Web Console von Kaspersky Security Center (auch Kaspersky Security Center Web Console genannt) installieren, wird standardmäßig automatisch ein Browser-Zertifikat für die Anwendung generiert. Sie können das automatisch generierte Zertifikat mit einem eigenen ersetzen.

Um das Zertifikat für Kaspersky Security Center Web Console mit einem eigenen zu ersetzen, gehen Sie wie folgt vor:

1. Öffnen Sie die Antwortdatei, die Sie bei der Installation von Kaspersky Security Center Web Console erstellt haben.

   Bei Bedarf können Sie ein neue Antwortdatei erstellen.

2. Geben Sie in der Datei die folgenden Pfade an:

   - Zur benutzerdefinierten Zertifikatsdatei von Kaspersky Security Center Web Console mithilfe des Parameters `certPath`.
   - Zum privaten Schlüssel, der mit dem benutzerdefinierten Zertifikat von Kaspersky Security Center Web Console verknüpft ist, mithilfe des Parameters `keyPath`.

     > Sie müssen beide Pfade angeben. Andernfalls informiert Sie der Webbrowser weiterhin darüber, dass Ihre Verbindung nicht privat ist.

3. Installieren Sie Kaspersky Security Center Web Console neu, indem Sie die neue Antwortdatei angeben. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie dieselbe Installationsdatei für Kaspersky Security Center Web Console verwenden möchten, entfernen Sie Kaspersky Security Center Web Console und installieren Sie anschließend die gleiche Version von Kaspersky Security Center Web Console.
   - Wenn Sie eine Installationsdatei einer aktualisierten Version verwenden möchten, führen Sie den Upgrade-Befehl aus.

Die Kaspersky Security Center Web Console verwendet jetzt das angegebene Zertifikat.

Konvertieren eines pfx-Zertifikats in ein pem-Zertifikat

Um in Kaspersky Security Center Web Console ein pfx-Zertifikat zu verwenden, müssen Sie dieses zunächst unter Verwendung eines beliebigen OpenSSL-basierten Cross-Plattform-Tools in ein pem-Format konvertieren.

So konvertieren Sie unter Linux ein pfx-Zertifikat in ein pem-Format:

1. Führen Sie in einem OpenSSL-basierten Cross-Plattform-Tool die folgenden Befehle aus:

   ```
   openssl pkcs12 -in <Dateiname.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <Dateiname.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Stellen Sie sicher, dass die Zertifikatsdatei und der private Schlüssel in dem gleichen Verzeichnis generiert werden, in dem sich die pfx-Datei befindet.

3. Kaspersky Security Center Web Console unterstützt keine kennwortgeschützten Zertifikate. Führen Sie daher in einem OpenSSL-basierten, plattformübergreifenden Tool den folgenden Befehl aus, um das Kennwort von der pem-Datei zu entfernen:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Verwenden Sie für die Input- und Output-Dateien nicht denselben Namen.

   Daraufhin ist die neue pem-Datei nicht mehr kennwortgeschützt. Um sie zu verwenden, muss kein Kennwort mehr eingegeben werden.

Die crt- und die pem-Datei sind bereit zur Verwendung. Sie können diese im Installer von Kaspersky Security Center Web Console angeben.

Szenario: Angeben des benutzerdefinierten Zertifikats des Administrationsservers

Sie können das benutzerdefinierte Zertifikat des Administrationsservers beispielsweise für eine bessere Integration in die vorhandene Public-Key-Infrastruktur (PKI) Ihres Unternehmens oder für eine benutzerdefinierte Konfiguration der Zertifikatfelder angeben. Es ist zweckmäßig, das Zertifikat sofort nach der Installation des Administrationsservers vor dem Abschluss des Schnellstartassistenten zu ersetzen.

> Die maximale Gültigkeitsdauer für jedes Zertifikat des Administrationsservers beträgt 397 Tage.

Erforderliche Vorrausetzungen

Dabei müssen die folgende Bedingungen erfüllt sein:

- Das neue Zertifikat muss im PKCS#12-Format erstellt werden (z. B. unter Verwendung der PKI des Unternehmens).
- Für das neue Zertifikat müssen die in der folgenden Tabelle aufgeführten Voraussetzungen erfüllt sein.

  Beachten Sie in der folgenden Tabelle die Anforderung "CA: true", die angibt, dass das neue Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority – CA) ausgestellt sein muss. Das neue Zertifikat mit der Anforderung "CA: true" muss die gesamte Vertrauenskette und einen privaten Schlüssel enthalten, welcher in einer Datei mit pfx- oder p12-Erweiterung gespeichert werden muss.

Voraussetzungen für die Zertifikate des Administrationsservers

Typ des Zertifikats	Voraussetzungen
Gewöhnliches Zertifikat, gewöhnliches Reservezertifikat ("C", "CR")	Minimale Schlüssellänge: 2048 Basic constraints: • Path Length Constraint: None Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, aber darf nicht kleiner als "1" sein. Schlüsselverwendung: • Digital signature • Certificate signing • Verschlüsselung des Schlüssels • CRL Signing Extended Key Usage (EKU): Serverauthentifizierung und Clientauthentifizierung. Die EKU ist optional, aber wenn Ihr Zertifikat diese enthält, müssen die Authentifizierungsdaten für Server und Client in der EKU angegeben werden. Das Zertifikat muss einen gültigen "Subject Alternative Name" (SAN) enthalten, der die Loopback-Adresse des Administrationsservers enthält: • Für IPv4: 127.0.0.1 • Für IPv6: 0:0:0:0:0:0:0:1
Mobilgerät-Zertifikat, Mobilgerät-Reservezertifikat ("M", "MR")	Minimale Schlüssellänge: 2048 Basic constraints: • CA: true • Path Length Constraint: None Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, wenn der Wert von Path Length Constraint des Common Certificates nicht kleiner als "1" ist. Schlüsselverwendung: • Digital signature • Certificate signing • Verschlüsselung des Schlüssels • CRL Signing Extended Key Usage (EKU): Serverauthentifizierung. Die EKU ist optional, aber wenn Ihr Zertifikat diese enthält, müssen die Authentifizierungsdaten des Servers in der EKU angegeben werden.
CA-Zertifikat für automatisch generierte Benutzerzertifikate ("MCA")	Minimale Schlüssellänge: 2048 Basic constraints: • CA: true • Path Length Constraint: None Der Wert von Path Length Constraint kann eine von "None" abweichende Integer-Zahl sein, wenn der Wert von Path Length Constraint des Common Certificates nicht kleiner als "1" ist. Schlüsselverwendung: • Digital signature • Certificate signing • Verschlüsselung des Schlüssels • CRL Signing Extended Key Usage (EKU): Clientauthentifizierung. Die EKU ist optional, aber wenn Ihr Zertifikat diese enthält, müssen die Authentifizierungsdaten des Clients in der EKU angegeben werden.

Von einer öffentlichen Zertifizierungsstelle ausgestellte Zertifikate verfügen nicht über die Berechtigung zum Signieren von Zertifikaten. Um solche Zertifikate zu verwenden, stellen Sie sicher, dass Sie den Administrationsagenten ab Version 13 auf den Verteilungspunkten oder Verbindungsgateways in Ihrem Netzwerk installiert haben. Andernfalls können Sie Zertifikate ohne die Berechtigung zum Signieren nicht verwenden.

Schritte

Das Angeben des Zertifikats des Administrationsservers erfolgt schrittweise:

1. **Ersetzen des Zertifikat des Administrationsservers**

   Verwenden Sie dafür das Befehlszeilendienstprogramm klsetsrvcert.

2. **Angeben eines neuen Zertifikats und Wiederherstellen der Verbindung der Administrationsagenten zum Administrationsserver**

   Wenn das Zertifikat ersetzt wird, verlieren alle Administrationsagenten, die zuvor mittels SSL mit Administrationsserver verbunden waren, die Verbindung zum Server und geben den Fehler "Fehler bei der Authentifizierung des Administrationsservers" zurück. Verwenden Sie das Befehlszeilendienstprogramm klmover, um das neue Zertifikat zu spezifizieren und die Verbindung wiederherzustellen.

3. **Angeben eines neuen Zertifikats in den Einstellungen der Kaspersky Security Center Web Console**

   Nachdem Sie das Zertifikat ersetzt haben, geben Sie es in der Antwortdatei an und aktualisieren Sie anschließend die Kaspersky Security Center Web Console unter Verwendung dieser Datei. Andernfalls kann die Kaspersky Security Center Web Console keine Verbindung zum Administrationsserver herstellen.

Ergebnisse

Wenn Sie das Szenario abgeschlossen haben, wurde das Zertifikat des Administrationsservers ersetzt und der Server wurde durch Administrationsagenten auf den Client-Geräten authentifiziert.

Zertifikats des Administrationsservers mittels Tool "klsetsrvcert" ersetzen

Um den Verlust der Kontrolle über die Geräte zu vermeiden, lesen Sie bitte folgendes Szenario, bevor Sie fortfahren: Szenario: Angeben des benutzerdefinierten Zertifikats des Administrationsservers.

So ersetzen Sie das Zertifikat des Administrationsservers:

Führen Sie aus der Befehlszeile das folgenden Dienstprogramm aus:

```
/opt/kaspersky/ksc64/sbin/klsetsrvcert [-t <certificate type> {-i <path to new certificate> [-p <password>] [-o
<validation parameters>] | -g <dns name>}][-f <replacement time>][-r <root certificates>][-l <log file path>]
```

Die Beschreibung der Parameter des Dienstprogramms klsetsrvcert finden Sie in der folgenden Tabelle.

Parameterwerte des Dienstprogramms klsetsrvcert

Parameter	Wert
`-t < Zertifikat-Typ >`	Typ des Zertifikats, das ersetzt werden muss. Mögliche Einstellungswerte des Parameters `< Zertifikat-Typ >`: • `C` – gewöhnliches Zertifikat für die Ports 13000 und 13291 ersetzen. • `CR` – gewöhnliches Reservezertifikat für die Ports 13000 und 13291 ersetzen.
`-f < Zeitpunkt des Ersetzens >`	Zeitplan für das Ersetzen der Zertifikate im Format "DD-MM-YYYY hh:mm" (für die Ports 13000 und 13291). Verwenden Sie diesen Parameter, wenn Sie das gemeinsame Zertifikat mit dem Reservezertifikat ersetzen möchten, bevor das gemeinsame Zertifikat abläuft. Geben Sie die Zeit an, zu der verwaltete Geräte mit dem Administrationsserver mit einem neuen Zertifikat synchronisiert werden müssen.
`-i < Pfad zum neuen Zertifikat >`	Container mit dem Zertifikat und privatem Schlüssel im Format PKCS#12 (Datei mit der p12- oder pfx-Erweiterung).
`-p < Kennwort >`	Kennwort, mithilfe dessen der p12-Container geschützt ist. Da das Zertifikat und ein privater Schlüssel im Container gespeichert werden, wird das Kennwort benötigt, um die Datei mit dem Container zu entschlüsseln.

Parameter	Wert
`-o < Validierungsparameter >`	Parameter der Zertifikatsvalidierung (durch Strichpunkt getrennt). Um ein benutzerdefiniertes Zertifikat ohne Signaturberechtigung zu verwenden, geben Sie im Dienstprogramm klsetsrvcert `-o NoCA` an. Dies ist nützlich für Zertifikate, die von einer öffentlichen Zertifizierungsstelle ausgestellt wurden. Um für Zertifikate vom Typ C oder CR die Länge des Chiffrierschlüssels zu ändern, geben Sie in dem Tool "klsetsrvcert" die Option `-o RsaKeyLen:< Schlüssellänge >` an, wobei der Parameter `< Schlüssellänge >` der erforderlichen Länge des Schlüssels entspricht. Andernfalls wird die aktuelle Länge des Zertifikatsschlüssels verwendet.
`-g < DNS-Name >`	Es wird ein neues Zertifikat für den angegebenen DNS-Namen (Common Name und Subject Alternative Name) erstellt.
`-r < Root-Zertifikate >`	Liste mit vertrauenswürdigen Zertifizierungsstellen für Stammzertifikate im Format PEM.
`-l < Pfad zur Protokolldatei >`	Datei zur Ausgabe der Ergebnisse. Standardmäßig erfolgt die Ausgabe im Standardausgabestream.

Um das benutzerdefinierte Zertifikat des Administrationsservers anzugeben, verwenden Sie beispielsweise den folgenden Befehl:

```
klsetsrvcert -t C -i <Pfad zum neuen Zertifikat> -p <Kennwort> -o NoCA
```

Nachdem das Zertifikat ersetzt wurde, verlieren alle Administrationsagenten, die über SSL mit dem Administrationsserver verbunden sind, ihre Verbindung. Verwenden Sie das Befehlszeilen-Dienstprogramm klmover, um es Wiederherstellen.

Um zu vermeiden, dass die Verbindungen mit den Administrationsagenten verloren gehen, verwenden Sie die folgenden Befehle:

1. Um ein neues Zertifikats zu installieren:

   ```
   klsetsrvcert -t CR -i <Pfad zum neuen Zertifikat> -p <Kennwort> -o NoCA
   ```

2. Um ein Datum anzugeben, an dem das Zertifikat angewendet wird:

   ```
   klsetsrvcert -f "DD-MM-YYYY hh:mm"
   ```

Wobei `DD-MM-YYYY hh:mm` das Datum 3-4 Wochen nach dem aktuellen Datum darstellt. Der zeitliche Versatz ist zum Austauschen des Zertifikats durch ein neues vorgesehen und ermöglicht die Verteilung dieses neuen Zertifikats an alle Administrationsagenten.

Fragen und Antworten

Welche zusätzlichen Schritte sind nach dem Austausch des allgemeinen Zertifikats des Administrationsservers erforderlich?

1. Stellen Sie sicher, dass die **Anforderungen für benutzerdefinierte Zertifikate erfüllt sind**.

   Wenn Sie anstelle des selbstsignierten Zertifikats ein benutzerdefiniertes Zertifikat verwenden, müssen Sie vor dem Upgrade von Kaspersky Security Center Linux auf die neuere Version sicherstellen, dass das Zertifikat den "Subject Alternative Name" (SAN) enthält. Wenn dies nicht der Fall ist, müssen Sie das Zertifikat unbedingt vor dem Upgrade von Kaspersky Security Center Linux ersetzen. Andernfalls können Sie sich nach dem Upgrade nicht mehr in der Webkonsole anmelden.

Um sicherzustellen, dass das Zertifikat den SAN enthält:

1. Führen Sie auf dem Gerät mit dem installierten Administrationsserver folgenden Befehl aus:

   - Für ein Linux-Gerät:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - Für ein Windows-Gerät:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Stellen Sie sicher, dass der "Subject Alternative Name" in der Befehlsausgabe angezeigt wird und die Adresse des Administrationsservergeräts enthält.

3. Falls der "Subject Alternative Name" nicht angezeigt wird, verwenden Sie das Tool klsetsrvcert, um Ihr benutzerdefiniertes Zertifikat durch ein Zertifikat zu ersetzen, dass die Anforderungen erfüllt.

2. Stellen Sie sicher, dass die Konfigurationsdatei des IAM-Servers die aktuelle Adresse des Administrationsservers enthält. Falls nicht, fügen Sie die Adresse zur Konfigurationsdatei hinzu.

3. Installieren Sie die Web Console erneut, um den folgenden Fehler zu vermeiden:

   Der Administrationsserver verwendet ein nicht vertrauenswürdiges Zertifikat. Bitte konfigurieren Sie die Anwendung neu, indem Sie ein gültiges Zertifikat angeben, oder wenden Sie sich an den Hauptadministrator.

Administrationsagenten mit dem Administrationsserver mittels Dienstprogramm klmover verbinden

Sie können Sie das Tool "klmover" verwenden, um unkontrollierte Geräte mit dem Administrationsserver zu verbinden. Dies kann beispielsweise erforderlich sein, wenn der Administrationsserver ausgefallen ist und nicht aus dem Backup wiederhergestellt werden kann.

Um die Verbindung wiederherzustellen, führen Sie das Tool "klmover" über die Befehlszeile aus:

- Unter Linux:

  - Für 32-Bit-Systeme: `/opt/kaspersky/klnagent/bin/klmover [-address <Serveradresse>] [-pn <Portnummer>] [-ps <SSL-Portnummer>] [-nossl] [-cert <Pfad zur Zertifikatsdatei>]`

  - Für 64-Bit-Systeme: `/opt/kaspersky/klnagent64/bin/klmover [-address <Serveradresse>] [-pn <Portnummer>] [-ps <SSL-Portnummer>] [-nossl] [-cert <Pfad zur Zertifikatsdatei>]`

- Unter Windows:

  - Für 32-Bit-Systeme: `<Pfad>\klmover.exe [-address <Serveradresse>] [-pn <Portnummer>] [-ps <SSL-Portnummer>] [-nossl] [-cert <Pfad zur Zertifikatsdatei>]`

  - Für 64-Bit-Systeme: `<Pfad>\klmover.exe [-address <Serveradresse>] [-pn <Portnummer>] [-ps <SSL-Portnummer>] [-nossl] [-cert <Pfad zur Zertifikatsdatei>]`

- Unter macOS:

  ```
  /Library/Application Support/Kaspersky Lab/klnagent/Binaries/klmover [-address <Serveradresse>] [-pn <Portnummer>] [-ps <SSL-Portnummer>] [-nossl] [-cert <Pfad zur Zertifikatsdatei>]
  ```

  wobei <Pfad> dem standardmäßigen Installationspfad des Administrationsagenten oder dem Installationspfad des Administrationsagenten entspricht, den Sie in den Einstellungen des Installationspakets des Administrationsagenten angegebenen haben.

Um zu verhindern, dass Angreifer Geräte aus dem Kontrollbereich Ihres Administrationsservers heraus verschieben können, wird es dringend empfohlen, für die Ausführung des Tools "klmover" den Kennwortschutz zu aktivieren. Um den Kennwortschutz zu aktivieren, wählen Sie in den Richtlinieneinstellungen des Administrationsagenten die Option **Deinstallationskennwort verwenden**.

Wenn Sie für einen kennwortgeschützten Administrationsagenten auf einem Gerät, das nicht mehr von Kaspersky Security Center Linux verwaltet wird, das Kennwort verlieren oder vergessen, können Sie diesen Administrationsagenten weder mit den Tools "klmover" und "Cleaner" (cleaner.exe) noch über die Eingabeaufforderung entfernen. In diesem Fall müssen Sie auf dem Gerät mit installiertem kennwortgeschützten Administrationsagenten das Betriebssystem neu installieren.

Das Tool "klmover" erfordert lokale Administratorrechte.

Das Aktivieren der Option **Deinstallationskennwort verwenden** aktiviert auf Windows-Geräten ebenfalls den Kennwortschutz für das Cleaner-Tool (cleaner.exe).

Sie können das Tool "klmover" nicht für Client-Geräte verwenden, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind. Für solche Geräte müssen Sie entweder den Administrationsagenten neu konfigurieren oder den Administrationsagenten neu installieren und das Verbindungs-Gateway angeben.

Die Beschreibung der Parameter des Dienstprogramms klmover finden Sie in der folgenden Tabelle.

Parameterwerte des Dienstprogramms klmover

Parameter	Wert
`-address <Serveradresse>`	Adresse des Administrationsservers für die Verbindung. Es kann die IP-Adresse oder der DNS-Name angegeben werden.
`-pn <Portnummer>`	Nummer des Ports, über den eine ungesicherte Verbindung zum Administrationsserver hergestellt wird. Standardmäßig wird Portnummer 14000 verwendet.
`-ps <SSL-Portnummer>`	Nummer des SSL-Ports, über den eine gesicherte Verbindung zum Administrationsserver mit dem SSL-Protokoll hergestellt wird. Standardmäßig wird Portnummer 13000 verwendet.
`-nossl`	Ungesicherte Verbindung zum Administrationsserver verwenden. Wenn kein Schlüssel verwendet wird, erfolgt die Verbindung des Administrationsagenten mit dem Administrationsserver über das SSL-Protokoll.
`-cert <Pfad zur Zertifikatsdatei>`	Angegebene Zertifikatsdatei für Authentifizierung am Administrationsserver verwenden.
`-nauninstpwd <Kennwort>`	Verwenden Sie diesen Parameter, um das Kennwort für die Deinstallation des Administrationsagenten anzugeben. Der Parameter ist nicht obligatorisch.

Neuausstellung des Webserver-Zertifikats

Das in Kaspersky Security Center Linux verwendete Zertifikat des Webservers wird sowohl für die Veröffentlichung von Installationspaketen des Administrationsagenten, die Sie anschließend auf Ihre verwalteten Geräte herunterladen, benötigt, als auch für die Veröffentlichung von iOS MDM-Profilen, iOS-Apps und Installationspaketen von Kaspersky Endpoint Security for Mobile. Abhängig von der aktuellen Programmkonfiguration können verschiedene Zertifikate als Webserver-Zertifikat fungieren (weitere Informationen finden Sie im Abschnitt Über die Zertifikate von Kaspersky Security Center Linux).

Möglicherweise müssen Sie das Webserver-Zertifikat erneut ausstellen, um die spezifischen Sicherheitsanforderungen Ihres Unternehmens zu erfüllen oder die kontinuierliche Verbindung Ihrer verwalteten Geräte aufrechtzuerhalten, bevor Sie mit dem Upgrade des Programms beginnen. Kaspersky Security Center Linux bietet zwei Möglichkeiten, das Webserver-Zertifikat neu auszustellen. Die Auswahl der Methode hängt davon ab, ob Sie mobile Geräte über das mobile Protokoll verbunden haben und verwalten (d. h. mithilfe des Mobilgerät-Zertifikats).

Wenn Sie im Abschnitt **Webserver** des Administrationsserver-Eigenschaftenfensters noch nie ein eigenes benutzerdefiniertes Zertifikat als Webserver-Zertifikat angegeben haben, dient das Mobilgerät-Zertifikat als Webserver-Zertifikat. In diesem Fall wird die Neuausstellung des Webserver-Zertifikats durch die Neuausstellung des mobilen Protokolls selbst durchgeführt.

So stellen Sie das Webserver-Zertifikat neu aus, wenn Sie mobile Geräte über das mobile Protokoll verwalten:

1. Generieren Sie Ihr benutzerdefiniertes Zertifikat und bereiten Sie es für die Verwendung in Kaspersky Security Center Linux vor. Prüfen Sie, ob Ihr benutzerdefiniertes Zertifikat die Anforderungen von Kaspersky Security Center Linux erfüllt. Ändern Sie das Zertifikat bei Bedarf.
2. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
3. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Webserver** aus.
4. Wählen Sie im Unterabschnitt **Über HTTP-Protokoll** die Option **Zertifikat aus Datei aktualisieren** aus und klicken Sie auf **Zertifikat ändern**.
5. Wählen Sie im folgenden Fenster im Feld **Format des Zertifikats** den Typ Ihres Zertifikats aus:

   - Wenn Sie **Container PKCS#12** ausgewählt haben, klicken Sie auf **Durchsuchen** neben dem Feld **Zertifikat** und geben Sie die Zertifikatsdatei auf Ihrer Festplatte an. Wenn die Zertifikatdatei kennwortgeschützt ist, geben Sie das Kennwort in das Feld **Kennwort** ein.
   - Wenn Sie **X.509-Zertifikat** ausgewählt haben, klicken Sie auf **Durchsuchen** neben dem Feld **Privater Schlüssel** und geben Sie den privaten Schlüssel auf Ihrer Festplatte an. Wenn der private Schlüssel kennwortgeschützt ist, geben Sie das Kennwort in das Feld **Kennwort** ein.
6. Klicken Sie auf **Speichern** und anschließend auf **OK**.

   Das Fenster wird geschlossen.
7. Ändern Sie bei Bedarf im Feld **HTTPS-Port des Webservers** die Nummer des HTTPS-Ports für den Webserver und klicken Sie auf **Speichern**.

Das Webserver-Zertifikat wird neu ausgestellt.

So stellen Sie das Webserver-Zertifikat neu aus, wenn Sie mobile Geräte nicht über das mobile Protokoll verwalten:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Zertifikate** aus.

3. Wenn Sie das von Kaspersky Security Center ausgestellte Zertifikat weiterhin verwenden möchten, gehen Sie wie folgt vor:

   a. Wählen Sie die Option **Das Zertifikat wurde mithilfe des Administrationsservers ausgestellt** aus und klicken Sie auf **Durchsuchen**.

   b. Wählen Sie im folgenden Fenster in der Einstellungsgruppe **Verbindungsadresse** und **Aktivierungsfrist** die entsprechenden Optionen aus und klicken Sie auf **OK**.

Wenn Sie alternativ Ihr eigenes benutzerdefiniertes Zertifikat verwenden möchten, gehen Sie wie folgt vor:

a. Prüfen Sie, ob Ihr benutzerdefiniertes Zertifikat die Anforderungen von Kaspersky Security Center Linux erfüllt. Ändern Sie das Zertifikat bei Bedarf.

b. Wählen Sie die Option **Anderes Zertifikat** aus, klicken Sie auf **Zertifikat verwalten** und klicken Sie im folgenden Fenster auf **Durchsuchen**.

c. Wählen Sie im folgenden Fenster im Feld **Format des Zertifikats** den Typ Ihres Zertifikats aus:

- Wenn Sie **Container PKCS#12** ausgewählt haben, klicken Sie auf **Durchsuchen** neben dem Feld **Zertifikat** und geben Sie die Zertifikatsdatei auf Ihrer Festplatte an. Wenn die Zertifikatsdatei kennwortgeschützt ist, geben Sie das Kennwort in das Feld **Kennwort** ein.
- Wenn Sie **X.509-Zertifikat** ausgewählt haben, klicken Sie auf **Durchsuchen** neben dem Feld **Privater Schlüssel** und geben Sie den privaten Schlüssel auf Ihrer Festplatte an. Wenn der private Schlüssel kennwortgeschützt ist, geben Sie das Kennwort in das Feld **Kennwort** ein.

d. Klicken Sie auf **Speichern** und anschließend auf **OK**.

Das Mobilgerät-Zertifikat wird erneut ausgestellt, um als Webserver-Zertifikat verwendet zu werden.

Das standardmäßige IAM-Zertifikats in ein benutzerdefiniertes Zertifikat ändern

So ändern Sie das standardmäßige IAM-Zertifikat:

1. Generieren Sie Ihr benutzerdefiniertes Zertifikat und bereiten Sie es für die Verwendung in Kaspersky Security Center Linux vor. Prüfen Sie, ob Ihr benutzerdefiniertes Zertifikat die Anforderungen von Kaspersky Security Center Linux erfüllt.

2. Stellen Sie sicher, dass die Gruppe "kladmins" Zugriff auf die Dateien der IAM-Zertifikate besitzt.

3. Öffnen Sie die IAM-Konfigurationsdatei unter `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

Fügen Sie in dieser Datei im Abschnitt `server_iam` die Pfade zum IAM-Zertifikat hinzu:

- `certificates.main.cert`: Pfad zur primären Zertifikatsdatei.
- `certificates.main.key`: Pfad zum privaten Schlüssel des primären Zertifikats. Der private Schlüssel darf nicht durch ein Kennwort geschützt sein.

4. Öffnen Sie die Konfigurationsdatei der Web Console unter `/etc/ksc-web-console-setup.json`

   Geben Sie in dieser Datei für das Feld `iamCertPath` den Pfad zum öffentlichen Schlüssel des primären Zertifikats an.

5. Starten Sie den Dienst "kliam" neu, indem Sie folgenden Befehl ausführen:

   ```
   sudo service kliam_srv restart
   ```

6. Installieren Sie die Web Console neu.

   Nach der Neuinstallation verwendet die Web Console das benutzerdefinierte IAM-Zertifikat.

So ändern Sie das IAM-Reserve-Zertifikat:

1. Öffnen Sie die IAM-Konfigurationsdatei unter `/var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml`

   Geben Sie in dieser Datei die Pfade zu den Dateien der IAM-Zertifikate an:

   - `server_iam.certificates.reserve.cert`: Pfad zur primären Zertifikatsdatei.
   - `server_iam.certificates.reserve.key`: Pfad zum privaten Schlüssel des primären Zertifikats. Der private Schlüssel darf nicht durch ein Kennwort geschützt sein.

2. Starten Sie den Dienst "kliam" neu, indem Sie folgenden Befehl ausführen:

   ```
   sudo systemctl restart kliam_srv.service
   ```

   Sobald die primäre Zertifikatsdatei abgelaufen ist, wird an dessen Stelle das IAM-Reserve-Zertifikat verwendet.

Adresse des Administrationsservers zur Konfiguration des IAM-Servers hinzufügen

Wenn das Common Certificate des Administrationsservers ("C") im Rahmen eines Upgrades, einer Standortänderung oder einer Migration geändert wurde, müssen Sie die Adresse des Administrationsservers in der Konfigurationsdatei des IAM-Servers angeben, um zwischen dem IAM-Server und dem Administrationsserver eine ordnungsgemäße Validierung des Zertifikats zu gewährleisten.

Um die Adresse des Administrationsservers zur Konfiguration des IAM-Servers hinzuzufügen:

1. Ermitteln Sie den "Subject Alternative Name" (SAN) vom Common Certificate des Administrationsservers ("C"), indem Sie den folgenden Befehl ausführen:

   ```
   sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
   ```

2. Führen Sie je nach Ausgabe des Befehls einen der folgenden Schritte aus:

   - Wenn Ausgabe indiziert, dass der Wert fehlt, überprüfen Sie die **Anforderungen an das benutzerdefinierte Zertifikat**.

     Wenn Sie anstelle des selbstsignierten Zertifikats ein benutzerdefiniertes Zertifikat verwenden, müssen Sie vor dem Upgrade von Kaspersky Security Center Linux auf die neuere Version sicherstellen, dass das Zertifikat den "Subject Alternative Name" (SAN) enthält. Wenn dies nicht der Fall ist, müssen Sie das Zertifikat unbedingt vor dem Upgrade von Kaspersky Security Center Linux ersetzen. Andernfalls können Sie sich nach dem Upgrade nicht mehr in der Webkonsole anmelden.

     Um sicherzustellen, dass das Zertifikat den SAN enthält:

     1. Führen Sie auf dem Gerät mit dem installierten Administrationsserver folgenden Befehl aus:

        - Für ein Linux-Gerät:

          ```
          sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
          ```

        - Für ein Windows-Gerät:

          ```
          certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
          ```

     2. Stellen Sie sicher, dass der "Subject Alternative Name" in der Befehlsausgabe angezeigt wird und die Adresse des Administrationsservergeräts enthält.

     3. Falls der "Subject Alternative Name" nicht angezeigt wird, verwenden Sie das Tool klsetsrvcert, um Ihr benutzerdefiniertes Zertifikat durch ein Zertifikat zu ersetzen, dass die Anforderungen erfüllt.

     Falls es die Anforderungen nicht erfüllt, ersetzen Sie das Common Certificate des Administrationsservers auf dem vorherigen Administrationsserver mithilfe des Tools "klsetsrvcert". Führen Sie anschließend die Aktualisierung, den Standortwechsel oder die Migration erneut durch.

   - Wenn der Wert mit dem Wert übereinstimmt, der während der Installation von Kaspersky Security Center Linux angegeben wurde (entweder im Schritt **IAM-Server-DNS-Namen eingeben** des Installationsassistenten oder als Parameter `KLSRV_UNATT_IAM_ADDRESS` bei der Installation im Silent-Modus), sind keine weiteren Maßnahmen mehr erforderlich. In diesem Fall interagieren der IAM-Server und der Administrationsserver interagieren ordnungsgemäß.

   - Wenn der Wert die Loopback-Adressen (127.0.0.1 und/oder 0:0:0:0:0:0:0:1) enthält, verwenden Sie eine davon in der Konfigurationsdatei. Es wird empfohlen, 127.0.0.1 zu verwenden.

3. Fügen Sie einen der SAN-Adresswerte aus dem Common Certificate des Administrationsservers dem Block `server_iam` in der Konfigurationsdatei des IAM-Servers im folgenden Format hinzu: `ksc_address: "<SAN_address>"`.

   Sie können die Konfigurationsdatei des IAM-Servers mit einem Texteditor (z. B. vi) bearbeiten. Der folgende Befehl öffnet die Datei im Texteditor vi:

   ```
   vi /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
   ```

   Beispiel für den Block "server_iam" in der Konfigurationsdatei des IAM-Servers:

   ```
   server_iam:
       iam_address: "ksc.example.com"
       server_display_name: "ksc.example.com"
       ksc_address: "oldksc.example.internal"
       ksc_ca: "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
   ```

Achten Sie darauf, die gleichen Abstände wie im Beispiel zu verwenden.

4. Überprüfen Sie, dass der Netzwerkname im Parameter `ksc_address` zur IP-Adresse des Administrationsservers aufgelöst wird. Dazu können Sie auf dem Administrationsserver den ping-Befehl verwenden.

   Wenn die aufgelöste Adresse abweicht, stellen Sie sicher, dass der alte Administrationsserver vom Netzwerk getrennt ist und dass keine DNS-Einträge mit der alten IP-Adresse mehr vorhanden sind. Wenn die Adresse nicht aufgelöst werden kann, ordnen Sie die Adresse mittels eines DNS-Eintrags in Ihrem Unternehmens-DNS hinzu oder fügen Sie einen Eintrag zur Datei "hosts" des Administrationsservers hinzu.

5. Starten Sie den Dienst des IAM-Servers neu, um die Konfigurationsänderungen anzuwenden. Führen Sie dazu folgenden Befehl aus:

```
sudo systemctl restart kliam_srv.service
```

Die Adresse des Administrationsservers wird der Konfigurationsdatei des IAM-Serves aus dem Common Certificate des Administrationsservers hinzugefügt.

Problemlösung

Konfigurationsprobleme auf dem IAM-Server können Fehler beim Anmelden an der Web Console verursachen. Die folgende Tabelle beschreibt mögliche Fehler und deren Lösungen.

Fehler	Beschreibung	Lösung
Ihre Anfrage kann momentan nicht verarbeitet werden. Bitte warten Sie und versuchen Sie es später erneut.	Zusätzlich zum Prozess der Dateninitialisierung nach einem Upgrade oder einer Wiederherstellung von Kaspersky Security Center Linux kann dieser Fehler auftreten, wenn die Verbindung zum Administrationsserver über die angegebene Netzwerkadresse fehlschlägt.	Überprüfen Sie mithilfe des ping-Befehls, zu welcher IP-Adresse der Netzwerkname aufgelöst wird.
Der Administrationsserver verwendet ein nicht vertrauenswürdiges Zertifikat. Bitte konfigurieren Sie die Anwendung neu, indem Sie ein gültiges Zertifikat angeben, oder wenden Sie sich an den Hauptadministrator.	Dieser Fehler kann auftreten, wenn der Adresswert in der Konfigurationsdatei des IAM-Servers nicht mit dem Wert im Attribut "Subject Alternative Name" (SAN) des Common Certificate des Administrationsservers übereinstimmt.	Befolgen Sie die obigen Anweisungen.
Der Benutzername oder das Kennwort ist falsch.	Neben falsch eingegebenen Anmeldeinformationen kann dieser Fehler auch dann auftreten, wenn in dem Netzwerk ein weiterer Administrationsserver mit dem gleichen Namen existiert.	Prüfen Sie, ob die angegebene Adresse zur IP-Adresse des aktuellen Administrationsservers aufgelöst wird.

Den freigegebenen Ordner angeben

Nach der Installation des Administrationsservers können Sie den Speicherort des freigegebenen Ordners in den Eigenschaften des Administrationsservers angeben. Standardmäßig wird der freigegebene Ordner auf dem Gerät mit dem Administrationsserver erstellt. In einigen Fällen (wie hohe Belastung oder die Notwendigkeit des Zugriffes aus einem isolierten Netzwerk) ist es jedoch zweckmäßig, den freigegebenen Ordner auf einer speziellen Dateiressource zu erstellen.

Der freigegebene Ordner wird in einigen Szenarien der Bereitstellung des Administrationsagenten verwendet.

Die Unterscheidung von Groß- und Kleinschreibung muss deaktiviert sein.

In der Kaspersky Security Center Web Console anmelden und abmelden

Sie können sich in der Kaspersky Security Center Web Console anmelden, nachdem Sie den Administrationsserver und den Server der Web Console installiert haben. Sie müssen die während der Installation angegebene Webadresse des Administrationsservers und den Port kennen (der Standard-Port ist 8080). In Ihrem Browser muss JavaScript aktiviert sein.

Sie können sich mit den folgenden Methoden an der Kaspersky Security Center Web Console anmelden:

- Mittels Domänenauthentifizierung (Single Sign-On)

  Diese Methode wird für die sichere Authentifizierung in Kaspersky Security Center Web Console verwendet, wenn diese mit einem Administrationsserver ab Version 16 verbunden ist. Wenn Sie die Domänenauthentifizierung verwenden möchten, müssen Sie während der Installation der Kaspersky Security Center Web Console zusätzliche Parameter für die Interaktion mit der Identitäts- und Zugriffsverwaltung (IAM) angeben.

- Durch Angeben von Name und Kennwort des Domänenbenutzers

  Bevor Sie sich unter Verwendung eines Domänenbenutzerkontos anmelden, fragen Sie den Domänencontroller ab, um die Liste der Domänenbenutzer abzurufen. Anschließend müssen Sie den Namen und das Kennwort des Domänenbenutzers angeben, um sich am Administrationsserver anzumelden. Diese Methode wird nur für die Authentifizierung mittels Microsoft Active Directory unterstützt.

- Durch Angeben von Namens und Kennwort des internen Benutzers

Das Benutzerkonto, mit dem Sie sich an der Kaspersky Security Center Web Console anmelden möchten, muss eine zugewiesene Rolle besitzen. Stellen Sie vor der Anmeldung sicher, dass der Domäne oder dem internen Benutzerkonto eine Rolle zugewiesen wurde. Andernfalls tritt ein Anmeldefehler auf.

Mittels Domänenauthentifizierung anmelden (Single Sign-On)

So melden Sie sich mittels Domänenauthentifizierung an der Kaspersky Security Center Web Console an:

1. Rufen Sie in Ihrem Browser die folgende Adresse auf: https://`<Adresse der Kaspersky Security Center Web Console>:<Port-Nummer>`.

   Die Seite zur Auswahl des Administrationsservers wird angezeigt.

2. Wenn Sie mehrere vertrauenswürdige Server hinzugefügt haben, wählen Sie in der Liste mit Administrationsservern den Administrationsserver aus, zu dem Sie eine Verbindung herstellen möchten.

   Wenn Sie nur einen einzigen Administrationsserver hinzugefügt haben, wird die Liste mit Administrationsservern nicht angezeigt.

   Der Browser wird auf folgende Adresse weitergeleitet: https://`<Administrationsserver-Adresse>`:4444

3. Konfigurieren Sie die Kerberos-Domänenauthentifizierung.

4. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie auf die Schaltfläche **Domänenauthentifizierung verwenden**.
   - Wenn auf dem Server mindestens ein virtueller Administrationsserver erstellt wurde und Sie sich an einem virtuellen Server mittels Domänenauthentifizierung anmelden möchten:

     a. Klicken Sie auf die Schaltfläche **Optionen des virtuellen Servers anzeigen**.

     b. Geben Sie den Namen des virtuellen Administrationsservers ein, den Sie während der Erstellung des virtuellen Servers angegeben haben.

     c. Klicken Sie auf die Schaltfläche **Domänenauthentifizierung verwenden**.

5. Geben Sie den Einmal-Sicherheitscode an, der von der Authentifizierungs-App auf dem Mobilgerät generiert wird.

   Konfigurieren Sie Zwei-Faktor-Authentifizierung bei der ersten Anmeldung für Ihr Konto. Wenn Ihnen die Konfiguration der Zwei-Faktor-Authentifizierung nicht zur Verfügung steht, wenden Sie sich an einen Benutzer, der über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** verfügt und konfigurierte Zwei-Faktor-Authentifizierung hat, um Ihr Konto zur Allow-Liste für Zwei-Faktor-Authentifizierung hinzuzufügen.

Nach der Anmeldung wird die Startseite von Kaspersky Security Center Web Console mit der Sprache und dem Design angezeigt, die Sie zuletzt verwendet haben. Sie können in der Kaspersky Security Center Web Console navigieren und sie bei Ihrer Arbeit mit Kaspersky Security Center Linux nutzen.

Durch Angabe von Name und Kennwort des Domänenbenutzers oder internen Benutzers anmelden

So melden Sie sich mittels Eingabe von Benutzernamen und Kennwort an der Kaspersky Security Center Web Console an:

1. Rufen Sie in Ihrem Browser die folgende Adresse auf: https://<Adresse der Kaspersky Security Center Web Console>:<Port-Nummer>.

   Die Seite zur Auswahl des Administrationsservers wird angezeigt.

2. Wenn Sie mehrere vertrauenswürdige Server hinzugefügt haben, wählen Sie in der Liste mit Administrationsservern den Administrationsserver aus, zu dem Sie eine Verbindung herstellen möchten.

   Wenn Sie nur einen einzigen Administrationsserver hinzugefügt haben, wird die Liste mit Administrationsservern nicht angezeigt.

   Der Browser wird auf folgende Adresse weitergeleitet: https://<Administrationsserver-Adresse>:4444

3. Führen Sie eine der folgenden Aktionen aus:

   - Um sich am Administrationsserver mit einem Domänen-Benutzerkonto anzumelden, geben Sie den Benutzernamen und das Kennwort des Domänenbenutzers ein.

     Sie können den Benutzernamen des Domänenbenutzers in einem der folgenden Formate eingeben:

     - `Benutzername@dns.domain`
     - `NTDOMAIN\Benutzername`

Bevor Sie sich mit dem Konto eines Domänenbenutzers anmelden, fragen Sie den Domänencontroller ab, um die Liste der Domänenbenutzer abzurufen.

- Um sich am Administrationsserver unter Angabe des Benutzernamens und des Kennworts des Administrators anzumelden, geben Sie den Benutzernamen und das Kennwort des internen Benutzers ein.
- Wenn auf dem Server mindestens ein virtueller Administrationsserver erstellt wurde und Sie sich an einem virtuellen Server anmelden möchten:

  a. Klicken Sie auf die Schaltfläche **Optionen des virtuellen Servers anzeigen**.

  b. Geben Sie den Namen des virtuellen Administrationsservers ein, den Sie während der Erstellung des virtuellen Servers angegeben haben.

  c. Geben Sie den Benutzernamen und das Passwort des Administrators ein, der die Berechtigungen für den virtuellen Administrationsserver besitzt.

4. Klicken Sie auf die Schaltfläche **Anmelden**.
5. Geben Sie den einmaligen Sicherheitscode an die von der Authentifizierungs-App auf dem Mobilgerät generiert wird.

   Konfigurieren Sie Zwei-Faktor-Authentifizierung bei der ersten Anmeldung für Ihr Konto. Wenn Ihnen die Konfiguration der Zwei-Faktor-Authentifizierung nicht zur Verfügung steht, wenden Sie sich an einen Benutzer, der über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** verfügt und konfigurierte Zwei-Faktor-Authentifizierung hat, um Ihr Konto zur Allow-Liste für Zwei-Faktor-Authentifizierung hinzuzufügen.
6. Wenn für Ihr Konto die erzwungene Kennwortänderung aktiviert ist oder Ihr Kennwort abgelaufen ist, wird das Fenster zur Kennwortänderung angezeigt. Legen Sie ein neues Kennwort fest, um sich an der Kaspersky Security Center Web Console anzumelden.

Nach der Anmeldung wird die Startseite von Kaspersky Security Center Web Console mit der Sprache und dem Design angezeigt, die Sie zuletzt verwendet haben. Sie können in der Kaspersky Security Center Web Console navigieren und sie bei Ihrer Arbeit mit Kaspersky Security Center Linux nutzen.

Abmelden

So melden Sie sich von einer laufenden Sitzung der Kaspersky Security Center Web Console ab:

Wechseln Sie im oberen Bereich zum Menü Ihres Benutzerkontos, indem Sie auf Ihren Kontonamen klicken, und wählen Sie anschließend **Abmelden**.

Kaspersky Security Center Web Console wird beendet und die Anmeldeseite wird angezeigt.

Benutzeroberfläche der Kaspersky Security Center Web Console

Kaspersky Security Center Linux wird über die Benutzeroberfläche von Kaspersky Security Center Web Console verwaltet.

Das Fenster der Kaspersky Security Center Web Console enthält die folgenden Elemente:

- Hauptmenü im linken Fensterbereich
- Oberer Bereich im oberen Teil des Fensters
- Arbeitsbereich im rechten Fensterbereich

Hauptmenü

Das Hauptmenü enthält die folgenden Abschnitte:

- **Administrationsserver**. Zeigt den Namen des Administrationsservers an, mit dem Sie aktuell verbunden sind. Sie können die Eigenschaften des Administrationsservers öffnen, indem Sie auf den Namen des Administrationsservers klicken.
- **Konsolen-Navigation**. Zeigt eine Übersicht des Hauptmenüs an. Die meisten der angezeigten Abschnitte können den Lesezeichen hinzugefügt oder als Startseite festgelegt werden. Der Abschnitt **Konsolen-Navigation** ist standardmäßig als Startseite eingestellt. Sie können diese Einstellung ändern.
- **Überwachung**. Bietet einen Überblick über Ihre Infrastruktur, den Schutzstatus und die Statistiken.
- **Asset-Verwaltung**. Enthält Tools für die Verwaltung von Geräten und Hardware sowie Richtlinien für Kaspersky-Anwendungen.
- **Aufgaben**. Enthält Tools zum Erstellen und Ausführen von Aufgaben.
- **Benutzer und Rollen**. Hier können Sie Benutzer und Rollen verwalten, Benutzerrechte durch Rollenzuweisung an Benutzer konfigurieren und Richtlinienprofile mit Rollen verknüpfen.
- **Datenverwaltung**. Bietet Ihnen Zugriff auf Datenverwaltungen der Anwendung.
- **Software-Verwaltung**. Hier können Sie neben den Anwendungen von Kaspersky und von Drittanbietern auch Installationspakete und Patches verwalten.
- **Vorgänge**. Enthält eine Vielzahl von Vorgängen wie die Anwendungslizenzierung und das Anzeigen und Verwalten von verschlüsselten Laufwerken und Verschlüsselungsereignissen.
- **Entdeckung und Bereitstellung**. Hier können Sie Netzwerkabfragen durchführen, um Client-Geräte zu finden, und diese Geräte manuell oder automatisch auf Administrationsgruppen verteilen. Dieser Abschnitt enthält außerdem den Schnellstartassistenten und den Assistenten für die Bereitstellung des Schutzes.
- **Marketplace**. Hier finden Sie Informationen über die Unternehmenslösungen von Kaspersky und können passende Lösungen auswählen und anschließend auf der Kaspersky-Website erwerben.
- **Einstellungen**. Hier können Sie ein Backup des aktuellen Zustands eines Web-Plug-ins anlegen, um den gespeicherten Zustand später wiederherzustellen. Enthält Ihre persönlichen Einstellungen für die Darstellung der Benutzeroberfläche, z. B. die gewählte Sprache für die Benutzeroberfläche oder das Farbschema.

Bei Bedarf können Sie das Hauptmenü durch Klicken auf das Chevron-Symbol (<<) am unteren Bildschirmrand minimieren.

Oberer Bereich

Der obere Bereich wird immer in allen Abschnitten der Konsole angezeigt und kann nicht ausgeblendet werden.

Die linke Seite des Bereichs enthält den Namen und das Logo der Anwendung. Wenn Sie auf den Namen oder das Logo der Anwendung klicken, öffnet sich die Startseite von Kaspersky Security Center Web Console.

Auf der rechten Seite des Fensters wird Folgendes angezeigt:

- Benachrichtigungssymbol (🔔). Wenn Sie das Symbol anklicken, öffnet sich ein Bereich mit Benachrichtigungen.
- Das Menü Ihres Benutzerkontos. Enthält einen Link zur Hilfe von Kaspersky Security Center Linux. Ferner können Sie sich hier von Kaspersky Security Center Linux abmelden, das Kennwort für Ihr Konto ändern und die Version von Kaspersky Security Center Web Console sowie die Liste der installierten Web-Plug-ins zur Verwaltung anzeigen.

Arbeitsbereich

Im Arbeitsbereich werden die Informationen zu den jeweiligen Abschnitten angezeigt, die Sie der Kaspersky Security Center Web Console anwählen. Er enthält außerdem Steuerelemente, mit denen Sie die Darstellung der Informationen anpassen können.

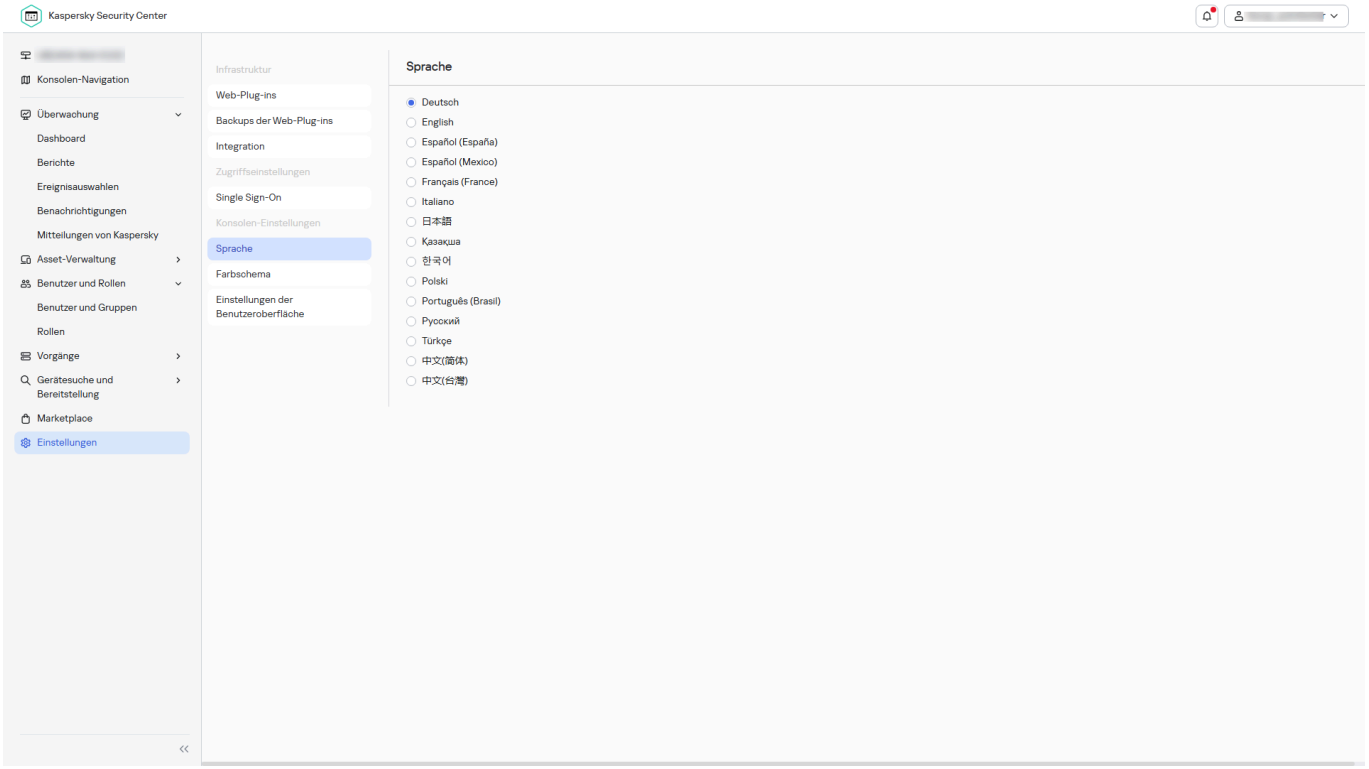
> Es wird empfohlen, für die Arbeit mit der Kaspersky Security Center Web Console nur einen Browser-Tab zu verwenden.

Sprache der Benutzeroberfläche von Kaspersky Security Center Web Console ändern

Sie können die Sprache der Benutzeroberfläche von Kaspersky Security Center Web Console auswählen.

So ändern Sie die Sprache der Benutzeroberfläche:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Sprache**.
2. Wählen Sie eine der unterstützten Lokalisierungssprachen aus.



Sprache der Benutzeroberfläche von Kaspersky Security Center Web Console ändern

Startseite der Kaspersky Security Center Web Console anpassen

Die Startseite wird angezeigt, nachdem Sie sich an der Kaspersky Security Center Web Console angemeldet haben.

Standardmäßig ist der Abschnitt **Konsolen-Navigation** als Startseite eingestellt. Bei Bedarf können Sie die Startseite anpassen.

So passen Sie die Startseite an:

1. Bewegen Sie im Abschnitt **Konsolen-Navigation** den Mauszeiger über das Element, das Sie als Startseite festlegen möchten.
2. Wenn das Homepage-Symbol (⌂) erscheint, klicken Sie es an.

Die Startseite ändert sich und es wird eine entsprechende Meldung auf dem Bildschirm angezeigt. Das als Startseite ausgewählte Element wird mit dem Homepage-Symbol (⌂) versehen.

Die Abschnitte **Marketplace** und **Einstellungen** können nicht als Startseite festgelegt werden.

Lesezeichen hinzufügen und entfernen

Sie können häufig aufgerufene Abschnitte von Kaspersky Security Center zu den Lesezeichen hinzuzufügen und diese anschließend über den Abschnitt **Lesezeichen** des Hauptmenüs schnell aufrufen.

Wenn Sie den Lesezeichen keinen Abschnitt hinzugefügt haben, wird der Abschnitt **Lesezeichen** im nicht Hauptmenü angezeigt.

Lesezeichen können für jene Abschnitte hinzugefügt werden, die Seiten enthalten und anzeigen. Wenn Sie beispielsweise den Abschnitt **Asset-Verwaltung** → **Assets (Geräte)** aufrufen, wird eine Seite mit der Gerätetabelle geöffnet. Dies bedeutet, dass Sie diesen Abschnitt den Lesezeichen hinzufügen können. Sollte jedoch nach der Auswahl eines Abschnitts im Hauptmenü ein Fenster oder gar kein Element angezeigt werden, können Sie diesen Abschnitt nicht zu den Lesezeichen hinzufügen.

So fügen Sie einen Abschnitt zu den Lesezeichen hinzu:

1. Bewegen Sie den Mauszeiger im Hauptmenü über den Abschnitt, den Sie hinzufügen möchten.
2. Wenn ein Lesezeichen-Symbol (🔖) erscheint, klicken Sie auf das Symbol.

   Der Abschnitt wird im Bereich **Lesezeichen** angezeigt.

So entfernen Sie einen Abschnitt aus den Lesezeichen:

1. Rufen Sie im Hauptmenü den Abschnitt **Lesezeichen** auf.
2. Bewegen Sie den Mauszeiger über den Abschnitt, den Sie entfernen möchten, und klicken Sie anschließend auf das Lesezeichen-Symbol (🔖).

   Der Abschnitt wird aus den Lesezeichen entfernt.

Sie können auch im Abschnitt **Konsolen-Navigation** Abschnitte zu den Lesezeichen hinzufügen, bzw. aus diesen entfernen. Bewegen Sie dazu den Mauszeiger über das gewünschte Element und klicken Sie auf das Lesezeichen-Symbol (🔖). Das ausgewählte Element wird mit dem Lesezeichen-Symbol (🔖) markiert und im Hauptmenü unter dem Abschnitt **Lesezeichen** angezeigt. Wenn Sie den Abschnitt aus den Lesezeichen entfernen möchten, klicken Sie auf das Lesezeichen-Symbol (🔖).

Der Abschnitt **Lesezeichen** wird nur im Hauptmenü angezeigt. Er wird nie auf der Seite **Konsolen-Navigation** angezeigt.

Kaspersky Security Center Web Console entfernen

In den folgenden Fällen müssen Sie möglicherweise den Kaspersky Security Center Web Console Server (auch Kaspersky Security Center Web Console genannt) entfernen:

- Beim Wiederherstellen von Daten aus einer Sicherung mit einem anderen Common Certificate.
- Beim erneuten Ausstellen des Common Certificate des Administrationsservers.
- Beim Ersetzen des Zertifikats der Web Console durch ein benutzerdefiniertes Zertifikat.
- Wenn die Kaspersky Security Center Web Console auf keinem Gerät mehr verwendet wird.

So entfernen Sie Kaspersky Security Center Web Console:

1. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:
   - `sudo dnf remove ksc-web-console`
   - `sudo apt remove ksc-web-console`
2. Das Ergebnis können Sie mit folgendem Befehl überprüfen:

   `sudo systemctl status KSC*`

   Die Kaspersky Security Center Web Console darf in der Befehlsausgabe nicht erscheinen.

Wenn Sie die Kaspersky Security Center Web Console wiederherstellen möchten, installieren Sie diese auf dem Gerät wie im Artikel Kaspersky Security Center Web Console installieren beschrieben.

Schnellstartassistent

Mit Kaspersky Security Center Linux können Sie eine minimale Auswahl von Einstellungen anpassen, die für den Aufbau eines zentralisierten Verwaltungssystems für den Schutz Ihres Netzwerks vor Bedrohungen erforderlich sind. Diese Konfiguration wird mithilfe des Schnellstartassistenten für das Programm durchgeführt. Während der Ausführung des Assistenten können Sie die folgenden Änderungen an der Anwendung vornehmen:

- Schlüsseldateien hinzufügen oder Aktivierungscodes eingeben, die automatisch auf die Geräte der Administrationsgruppen verteilt werden können.
- Einrichten des Versands von E-Mails zur Benachrichtigungen über Ereignisse, die während der Ausführung des Administrationsservers und der verwalteten Anwendungen auftreten.
- Schutzrichtlinien für Workstations und Server sowie Aufgaben zur Schadsoftware-Untersuchung, Update-Download und zum Daten-Backup für die oberste Hierarchieebene der verwalteten Geräte erstellen.

  Der Schnellstartassistent erstellt Richtlinien nur für die Anwendungen, deren Ordner **Assets (Geräte)** noch keine Richtlinien enthält. Der Schnellstartassistent erstellt keine Aufgaben, deren Namen mit den Aufgabennamen übereinstimmen, die für die obere Hierarchieebene der verwalteten Geräte bereits erstellt wurden.

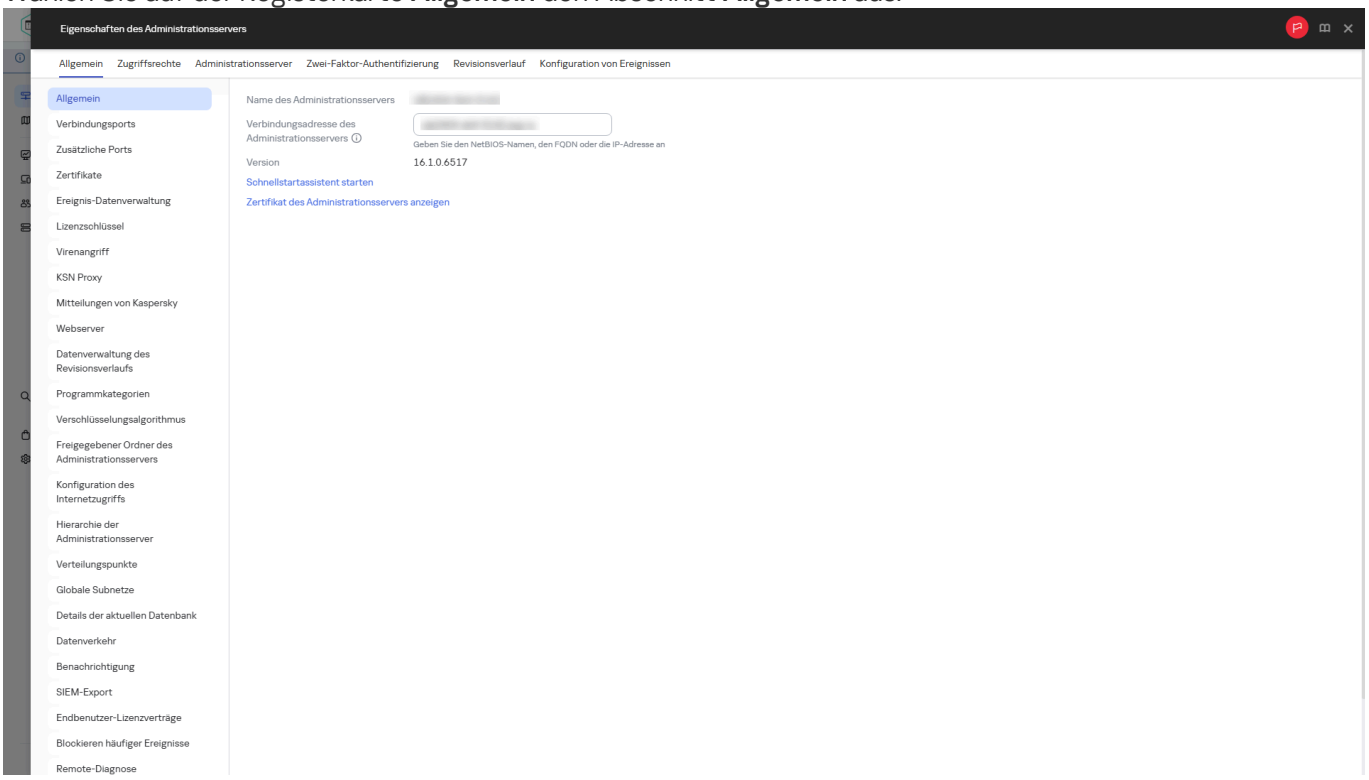
Die Anwendung schlägt automatisch vor, beim ersten Verbindungsaufbau zum Server nach der Installation des Administrationsservers den Schnellstartassistenten zu starten. Sie können den Schnellstartassistenten auch jederzeit manuell starten.

So starten Sie den Schnellstartassistenten manuell:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Allgemein** aus.



Eigenschaftenfenster des Administrationsservers

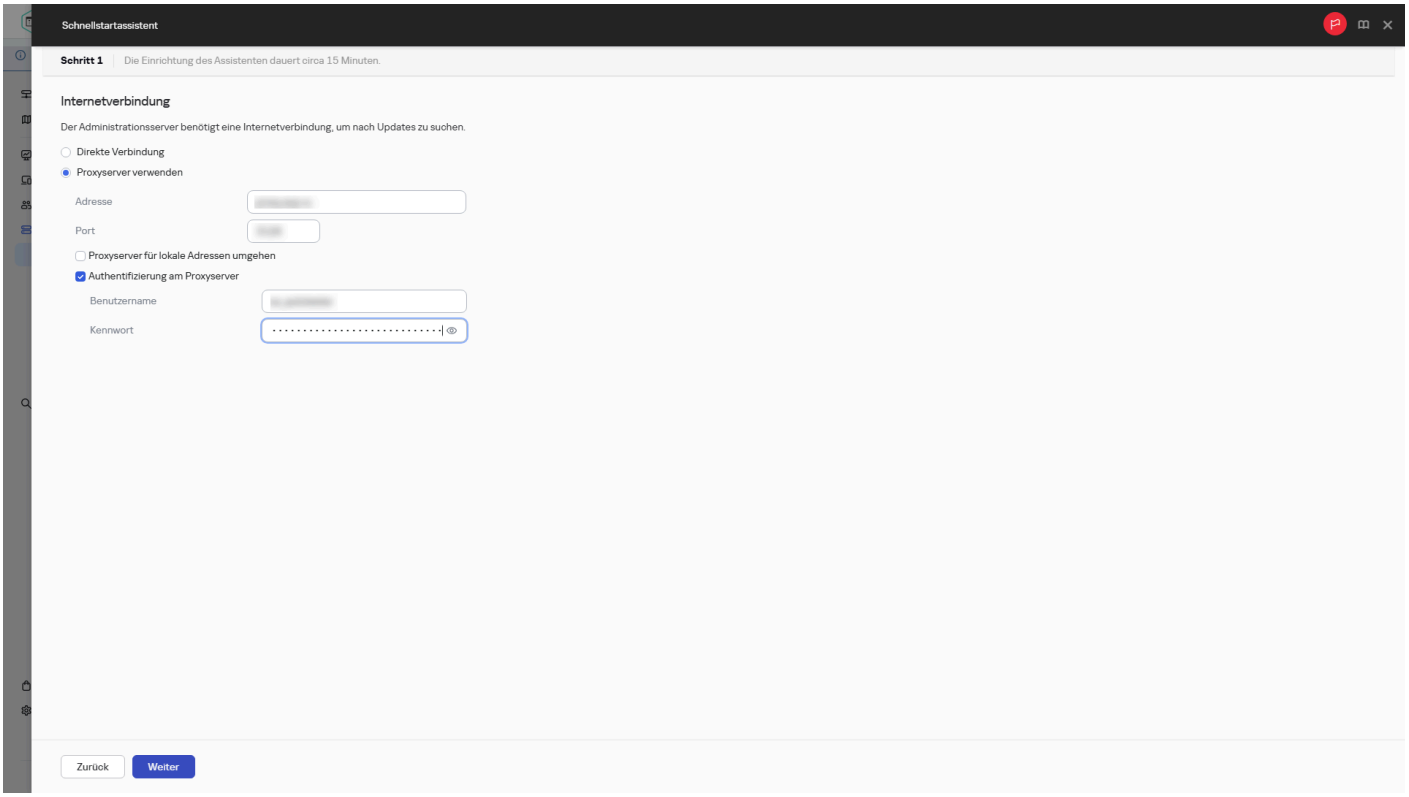
3. Klicken Sie auf die Schaltfläche **Schnellstartassistent starten**.

   Der Assistent schlägt vor, die ursprünglichen Einstellungen des Administrationsservers zu generieren. Folgen Sie den Anweisungen des Assistenten. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

Schritt 1. Einstellungen für die Internetverbindung festlegen

Geben Sie die Internetzugriffseinstellungen für den Administrationsserver an. Sie müssen den Internetzugang anpassen, um Kaspersky Security Network zu verwenden und um Updates für die Antiviren-Datenbanken von Kaspersky Security Center Linux und die verwalteten Kaspersky-Anwendungen herunterzuladen.

Aktivieren Sie die Option **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung benutzen wollen. Wenn die Option aktiviert ist, sind die Eingabefelder der Einstellungen verfügbar. Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:



Einstellungen der Internetverbindung

- **Adresse**

  Die Proxyserver-Adresse für die Verbindung von Kaspersky Security Center Linux mit dem Internet.

- **Port**

  Nummer des Ports, über den die Proxy-Verbindung zu Kaspersky Security Center Linux hergestellt wird.

- **Proxyserver für lokale Adressen umgehen**

  Bei der Verbindung mit den Geräten im lokalen Netzwerk wird kein Proxyserver verwendet.

- **Authentifizierung am Proxyserver**

  Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

  Die Eingabefelder sind verfügbar, wenn das Kontrollkästchen **Proxyserver verwenden** aktiviert ist.

- **Benutzername**

  Benutzerkonto, unter dem die Verbindung zum Proxyserver hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

- **Kennwort**

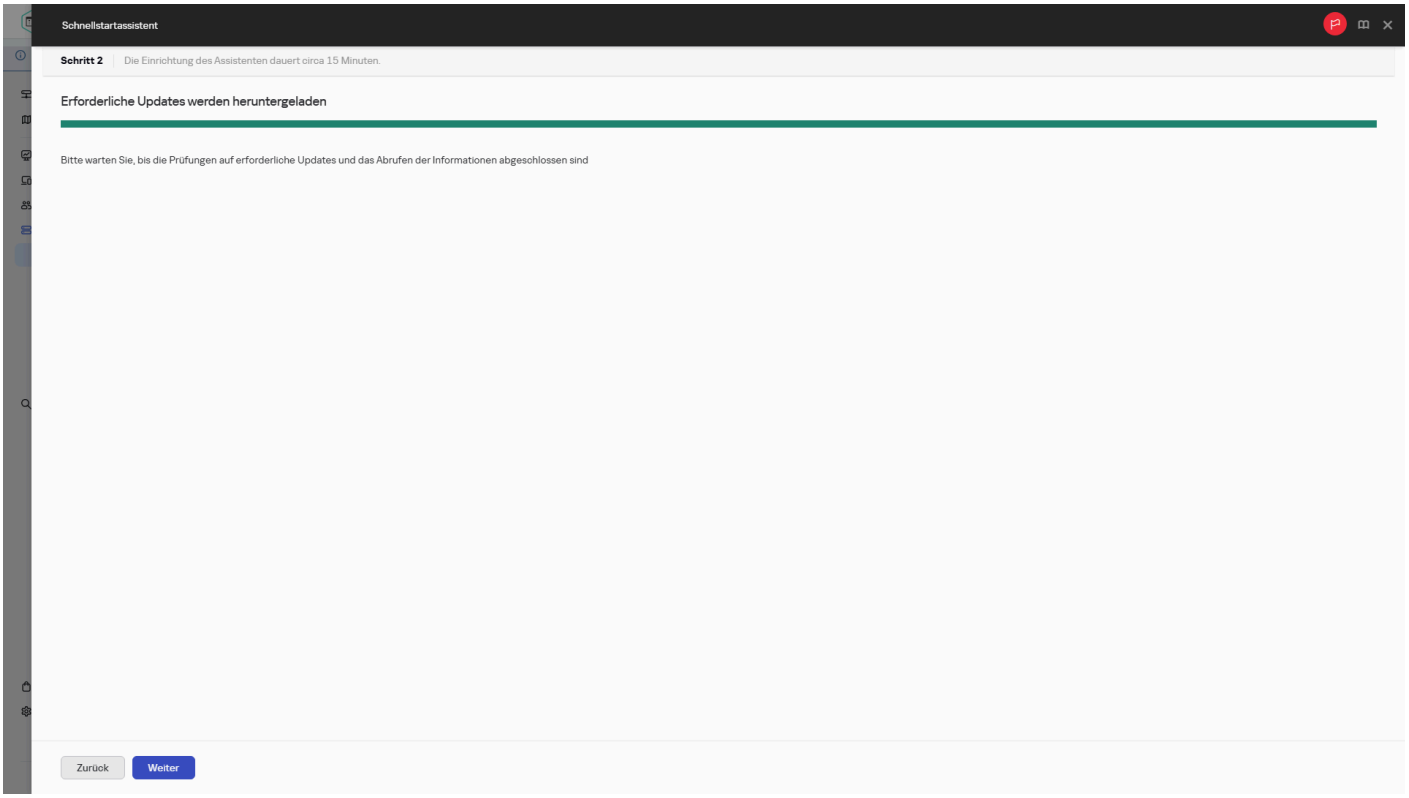
  Kennwort, das von dem Benutzer festgelegt wird, unter dessen Benutzerkonto die Proxyserver-Verbindung hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie diese für die erforderliche Zeitspanne gedrückt.

Das Konfigurieren des Internetzugriffs ist auch später, unabhängig vom Schnellstartassistenten, möglich.

Schritt 2. Erforderliche Updates herunterladen

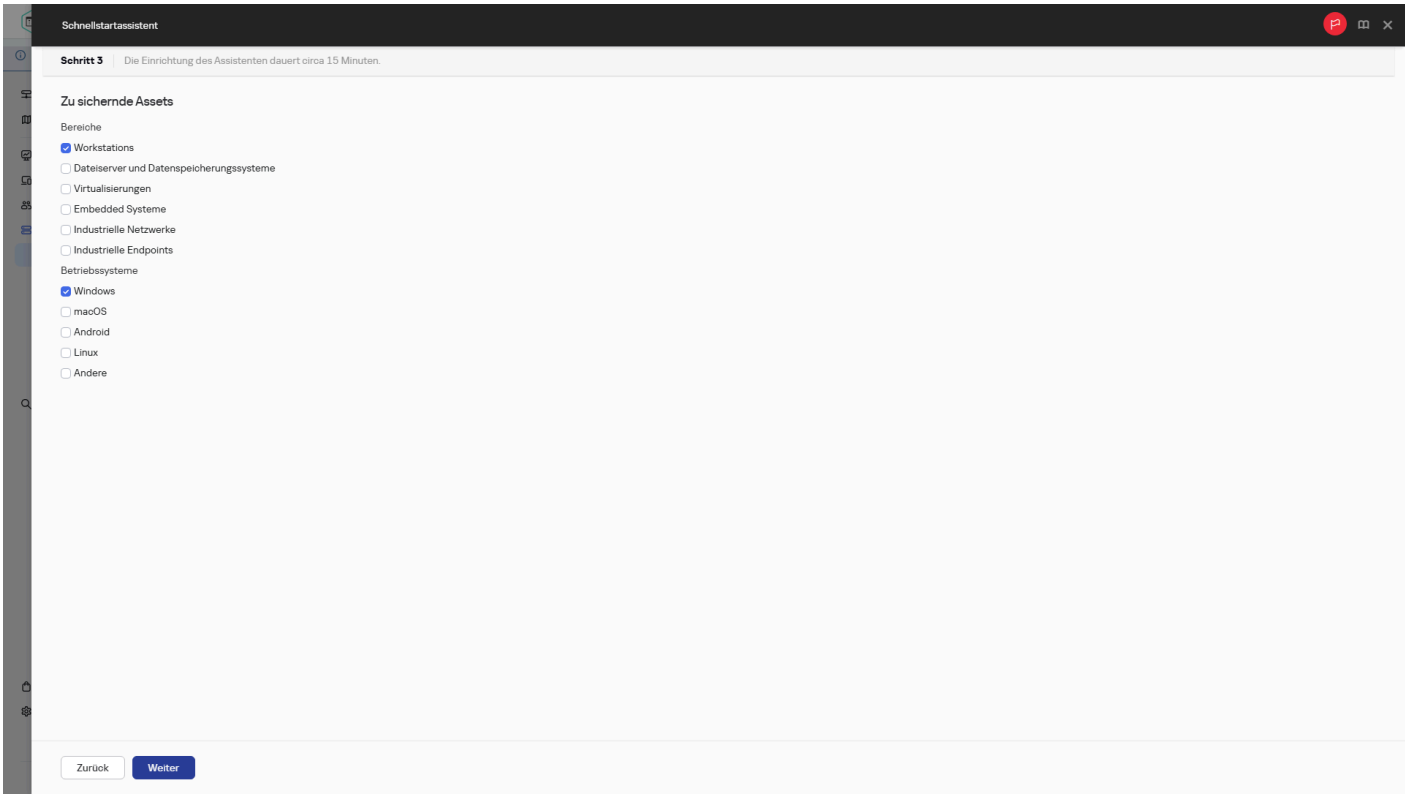
Die erforderlichen Updates werden automatisch von den Kaspersky-Servern heruntergeladen.



Erforderliche Updates herunterladen

Schritt 3. Zu sichernde Assets auswählen

Wählen Sie die Schutzbereiche und Betriebssysteme aus, die Sie in Ihrem Netzwerk verwenden. Geben Sie bei der Auswahl die Filter für die Plug-ins zur Anwendungsverwaltung und für die Programmpakete auf den Kaspersky-Servern an, die Sie herunterladen und auf Client-Geräten in Ihrem Netzwerk installieren können.



Zu sichernde Assets auswählen

Wählen Sie die Optionen aus:

- **Bereiche**

  Sie können die folgenden Schutzbereiche auswählen:

  - **Workstations**
  - **Dateiserver und Datenspeicherungssysteme**
  - **Virtualisierung**
  - **Eingebettete Systeme**
  - **Industrielle Netzwerke**
  - **Industrielle Endpunkte**

- **Betriebssysteme**

  Sie können die folgende Plattformen auswählen:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Sonstige

  Informationen zu den unterstützten Betriebssystemen finden Sie im Abschnitt "Hardware- und Softwarevoraussetzungen für die Kaspersky Security Center Web Console".

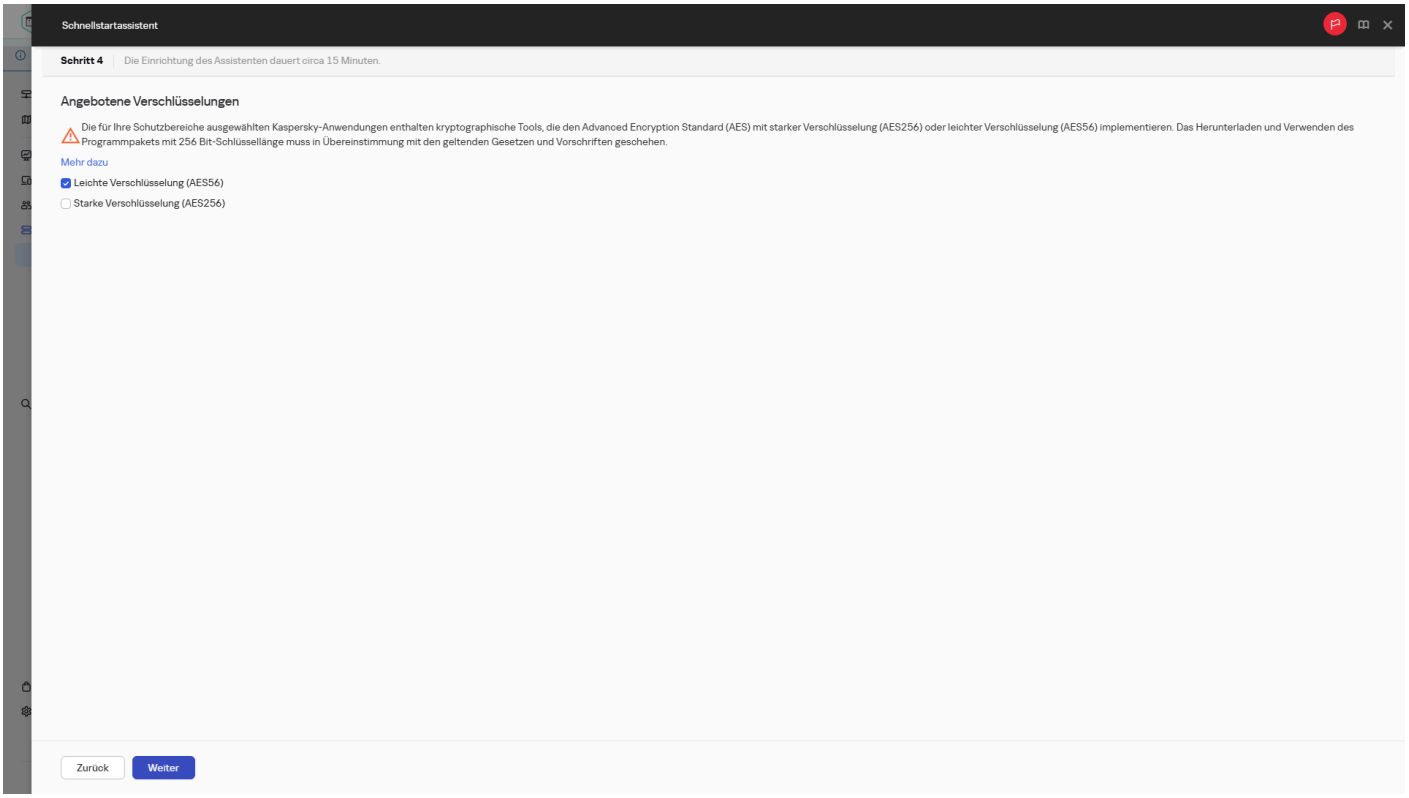
Die Pakete für Kaspersky-Anwendungen können auch später aus der Liste der verfügbaren Pakete ausgewählt werden, ohne den Schnellstartassistenten zu verwenden. Um die Suche nach den benötigten Paketen zu vereinfachen, können Sie die Liste der verfügbaren Pakete nach verschiedenen Kriterien filtern.

Schritt 4. Verwendete Verschlüsselung für die Lösungen auswählen

Das Fenster **Angebotene Verschlüsselungen** wird nur angezeigt, wenn Sie **Workstations** als einen Schutzbereich ausgewählt haben.

Kaspersky Endpoint Security für Windows enthält Verschlüsselungs-Tools für die Informationen, die auf Windows-basierten Client-Geräten gespeichert werden. Diese Tools Verschlüsselungswerkzeuge, die den Advanced Encryption Standard (AES) mit einer 256-Bit oder 56-Bit Schlüssellänge implementiert haben.

Das Herunterladen und die Verwendung des Programmpakets mit einer 256-Bit-Schlüssellänge muss in Übereinstimmung mit den geltenden Gesetzen und Vorschriften erfolgen. Um ein Programmpaket von Kaspersky Endpoint Security für Windows herunterzuladen, dass den Bedürfnissen Ihrer Organisation entspricht, konsultieren Sie die Gesetzgebung in dem Land, in dem sich die Client-Geräte Ihrer Organisation befinden.



Verwendete Verschlüsselung für die Lösungen auswählen

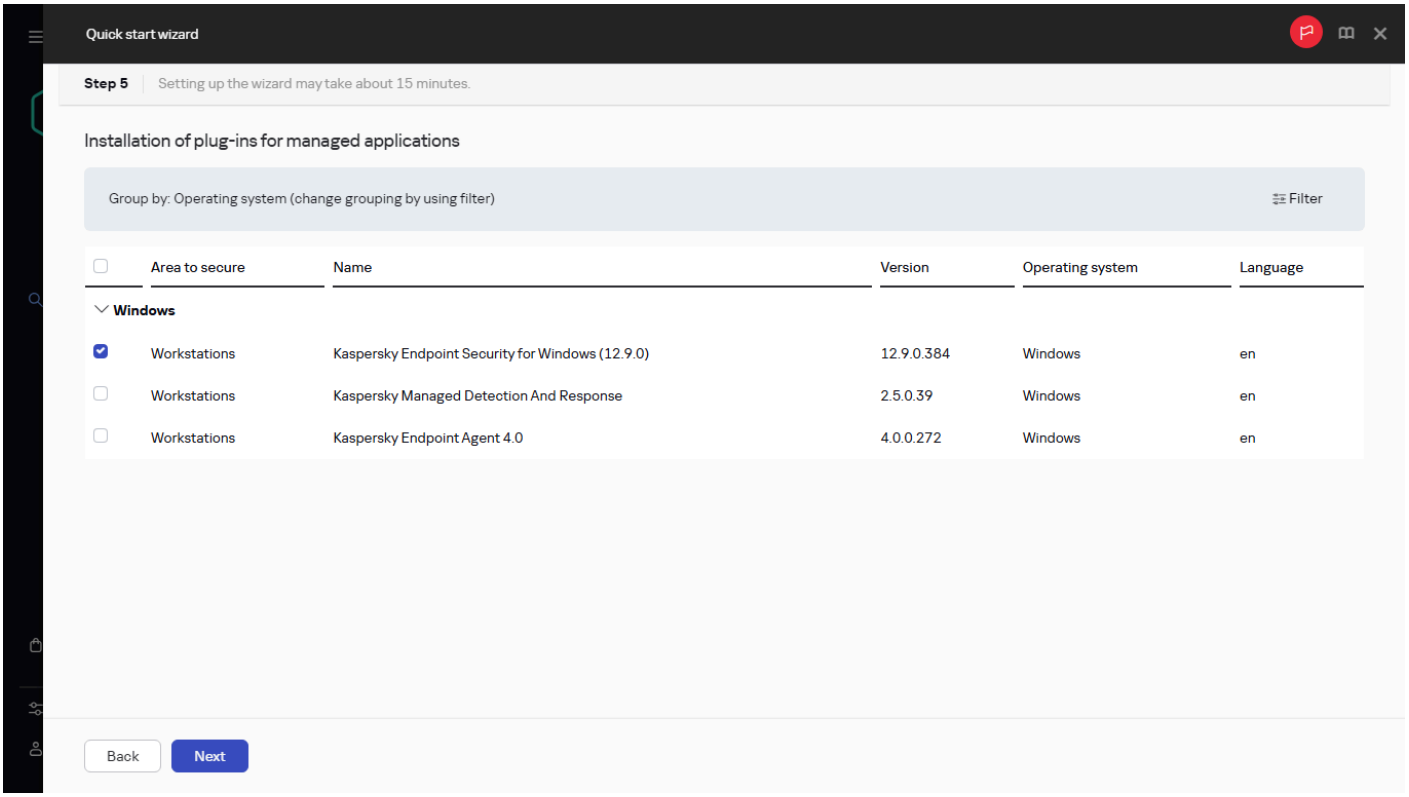
Wählen Sie im Fenster **Angebotene Verschlüsselungen** einen der folgenden Verschlüsselungs-Typen aus:

- Leichte Verschlüsselung. Dieser Verschlüsselungstyp verwendet eine 56-Bit-Schlüssellänge.
- Starke Verschlüsselung. Dieser Verschlüsselungstyp verwendet eine 256-Bit-Schlüssellänge.

Das Auswählen der Programmpakete für Kaspersky Endpoint Security für Windows mit erforderlichem Verschlüsselungstyp kann später, unabhängig vom Schnellstartassistenten, durchgeführt werden.

Schritt 5. Plug-ins für verwaltete Programme konfigurieren

Auswahl der zu installierenden Plug-ins für verwaltete Anwendungen. Eine Liste aller auf Kaspersky-Servern befindlichen Plug-ins wird angezeigt. Die Liste wird nach den Optionen gefiltert, die beim vorherigen Schritt des Assistenten ausgewählt wurden. Standardmäßig enthält eine komplette Liste Plug-ins aller Sprachen. Um nur die Plug-ins einer bestimmten Sprache anzuzeigen, nutzen Sie den Filter.



Plug-ins für verwaltete Programme installieren

Die Liste der Plug-ins umfasst die folgenden Spalten:

- **Schutzbereich**

  Die ausgewählten Bereiche, die geschützt werden sollen, werden in dieser Spalte angezeigt.

- **Typ**

  In dieser Spalte werden die Plug-in-Typen angezeigt.

- **Name**

  Die Auswahl der Plug-ins richtet sich nach den Schutzbereichen und Plattformen, die Sie beim vorhergehenden Schritt ausgewählt haben.

- **Version**

  Die Liste enthält Plug-ins aller auf Kaspersky-Servern befindlichen Versionen. Standardmäßig sind die Plug-ins der aktuellsten Versionen ausgewählt.

- **Neueste Version**

  In dieser Spalte wird angezeigt, ob die Version des Plug-ins aktuell ist. Wenn der Wert **true** angezeigt wird, handelt es sich bei dem entsprechenden Plug-in um die neueste Version. Wenn der Wert **false** angezeigt wird, existiert von dem entsprechenden Plug-in eine aktuellere Version.

- **Betriebssystem**

  In dieser Spalte werden die Betriebssysteme der Plug-ins angezeigt.

- **Sprache**

  Standardmäßig wird die Lokalisierungssprache eines Plug-ins durch die Sprache von Kaspersky Security Center Linux vorgegeben, die Sie während der Installation ausgewählt haben. In der Dropdown-Liste **Anzeige der Sprache der Verwaltungskonsole oder** können Sie andere Sprachen angeben.

Klicken Sie nach dem Auswählen der Plug-ins auf **Weiter**, um die Installation zu beginnen.

Sie können die Installation der Verwaltungs-Plug-ins für Kaspersky-Anwendungen manuell, unabhängig vom Schnellstartassistenten, durchführen.

Der Schnellstartassistent installiert die ausgewählten Plug-ins automatisch. Für die Installation einiger Plug-ins müssen Sie die Bestimmungen der EULA akzeptierten. Lesen Sie den angezeigten EULA-Text, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** und klicken Sie auf die Schaltfläche **Installieren**. Wenn Sie die Bestimmungen der EULA nicht akzeptieren, wird das Plug-in nicht installiert.

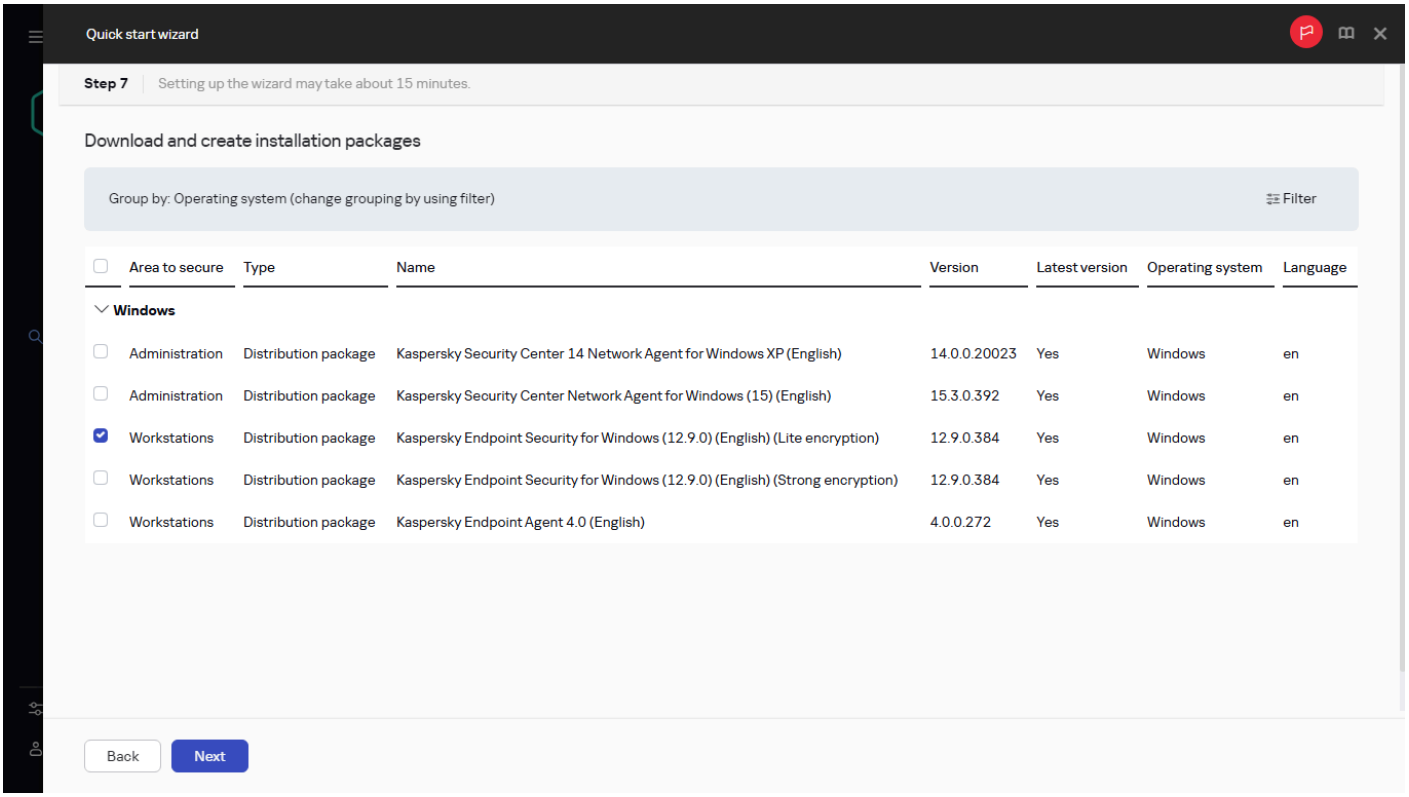
Wenn alle ausgewählten Plug-ins installiert wurden, geht der Schnellstartassistent automatisch zum nächsten Schritt über.

Schritt 6. Programmpakete herunterladen und Installationspakete erstellen

Wählen Sie das herunterzuladende Programmpaket.

Für Pakete verwalteter Anwendungen muss möglicherweise eine bestimmte Mindestversion von Kaspersky Security Center Linux installiert werden.

Nachdem Sie den Verschlüsselungstyp für Kaspersky Endpoint Security für Windows ausgewählt haben, wird eine Liste von Programmpaketen mit beiden Verschlüsselungstypen angezeigt. In der Liste ist ein Programmpaket mit dem ausgewählten Verschlüsselungstyp ausgewählt. Sie können Programmpakete eines beliebigen Verschlüsselungstyps auswählen. Die Sprache des Programmpakets entspricht der Sprache von Kaspersky Security Center Linux. Wenn kein Programmpaket für die Sprache von Kaspersky Security Center Linux vorhanden ist, wird das englische Verteilungspaket ausgewählt.



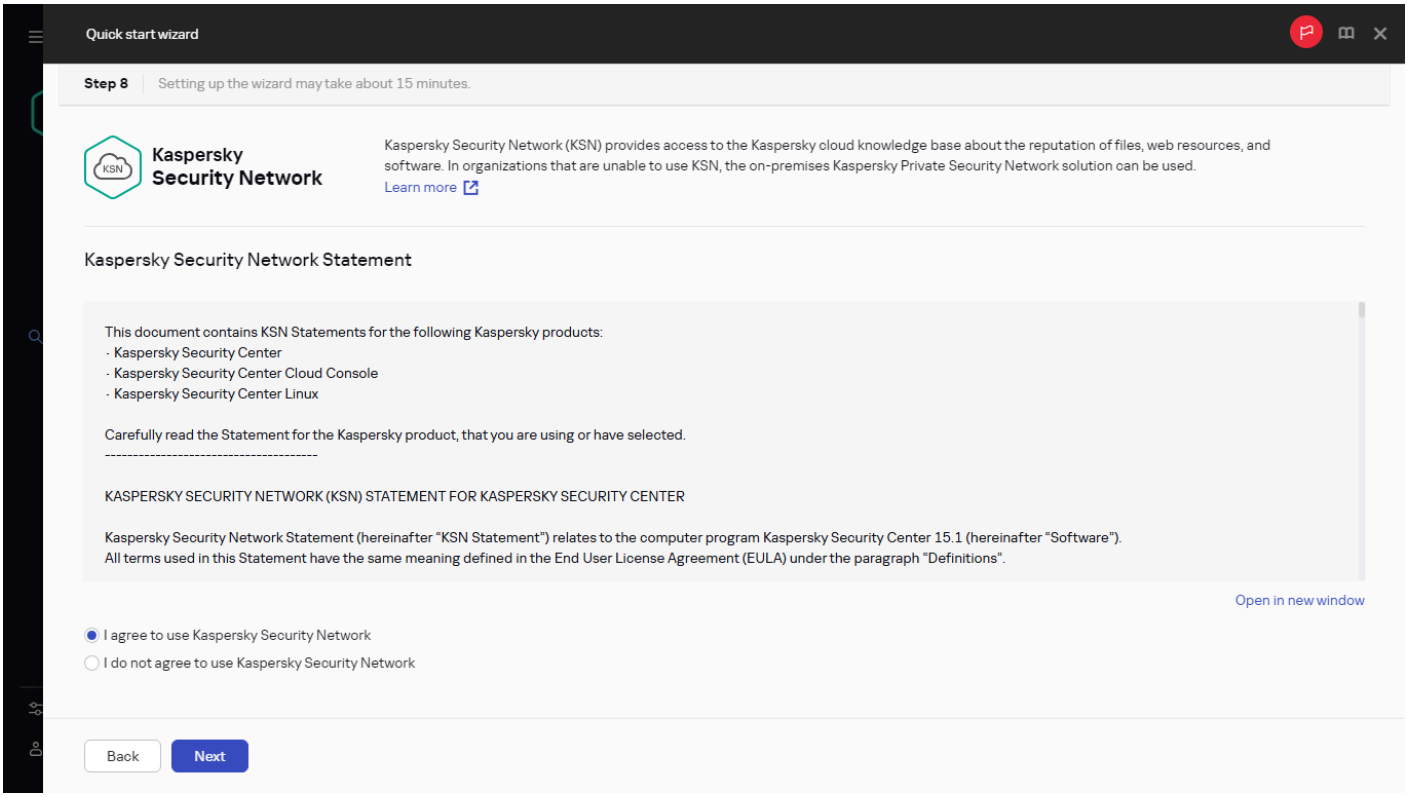
Programmpakete herunterladen und Installationspakete erstellen

Um den Download einiger Programmpakete abzuschließen, müssen Sie die EULA akzeptieren. Wenn Sie auf die Schaltfläche **Akzeptieren** klicken, wird der EULA-Text angezeigt. Um zum nächsten Schritt des Assistenten zu wechseln, müssen Sie die Bestimmungen und Bedingungen der EULA und die Bestimmungen und Bedingungen der Kaspersky-Datenschutzrichtlinie akzeptieren. Wenn Sie die Bestimmungen und Bedingungen nicht akzeptieren, wird der Download des Pakets abgebrochen.

Nachdem Sie die Bestimmungen und Bedingungen der EULA und die Bestimmungen und Bedingungen der Kaspersky-Datenschutzrichtlinie akzeptiert haben, wird der Download des Programmpakets fortgesetzt. Die Installationspakete können Sie später verwenden, um Kaspersky-Anwendungen auf Client-Geräten bereitzustellen.

Schritt 7. Kaspersky Security Network konfigurieren

Legen Sie die Einstellungen für die Übertragung von Informationen über die Ausführung von Kaspersky Security Center Linux in die Wissensdatenbank von Kaspersky Security Network fest.



Kaspersky Security Network konfigurieren

Wählen Sie eine der folgenden Varianten aus:

- **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network**

  Kaspersky Security Center Linux und die verwalteten Anwendungen, die auf Client-Geräten installiert sind, übertragen ihre Vorgangsdetails automatisch an Kaspersky Security Network. Die Zusammenarbeit mit Kaspersky Security Network gewährleistet ein schnelleres Datenbanken-Update mit Daten über Viren und Bedrohungen, wodurch die Reaktionsgeschwindigkeit auf neue Sicherheitsgefährdungen erhöht wird.

- **Ich lehne die Nutzungsbedingungen von Kaspersky Security Network ab**

  Kaspersky Security Center Linux und verwaltete Anwendungen senden keine Informationen an Kaspersky Security Network.

  Wenn Sie diese Option auswählen, wird die Verwendung von Kaspersky Security Network deaktiviert.

Sie können den Zugriff auf Kaspersky Security Network (KSN) später einrichten, unabhängig vom Schnellstartassistenten.

Schritt 8. Methode zur Programmaktivierung auswählen

Wählen Sie eine der folgenden Varianten zur Aktivierung von Kaspersky Security Center Linux aus:

- **Durch Eingabe Ihres Aktivierungscodes**

  Der *Aktivierungscode* ist eine eindeutige Zeichenfolge aus 20 Buchstaben und Ziffern. Den Aktivierungscode geben Sie ein, um einen Schlüssel zur Aktivierung von Kaspersky Security Center Linux hinzuzufügen. Sie erhalten den Aktivierungscode an die E-Mail-Adresse, die Sie beim Kauf von Kaspersky Security Center angegeben haben.

  Um die Anwendung unter Verwendung eines Aktivierungscodes zu aktivieren, ist ein Internetzugang für die Verbindung mit den Aktivierungsservern von Kaspersky erforderlich.

  Wenn Sie diese Aktivierungsoption ausgewählt haben, können Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** aktivieren.

  Wenn diese Option aktiviert ist, wird der Lizenzschlüssel automatisch an die verwalteten Geräte verteilt.

  Wenn diese Option deaktiviert ist, können Sie den Lizenzschlüssel später im Abschnitt **Vorgänge** → **Lizenzierung** → **Lizenzen** des Hauptmenüs an die verwalteten Geräte bereitstellen.

- **Schlüsseldatei angeben**

  Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky erhalten. Die Schlüsseldatei dient dazu, einen Schlüssel für die Aktivierung der Anwendung hinzuzufügen.

  Sie erhalten Ihre Schlüsseldatei an die E-Mail-Adresse, die Sie beim Kauf von Kaspersky Security Center angegeben haben.

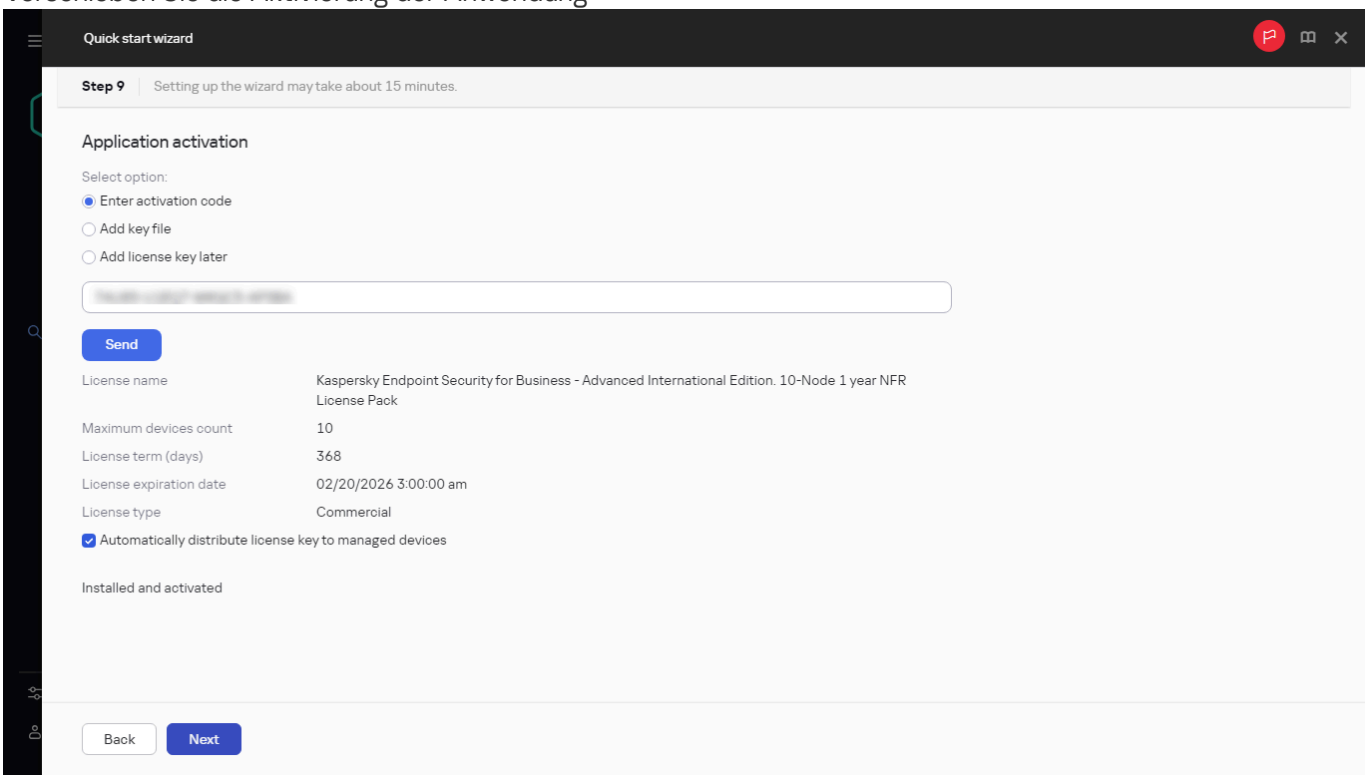
  Um die Anwendung mit einer Schlüsseldatei zu aktivieren, ist keine Verbindung mit den Aktivierungsservern von Kaspersky erforderlich.

  Wenn Sie diese Aktivierungsoption ausgewählt haben, können Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** aktivieren.

  Wenn diese Option aktiviert ist, wird der Lizenzschlüssel automatisch an die verwalteten Geräte verteilt.

  Wenn diese Option deaktiviert ist, können Sie den Lizenzschlüssel später im Abschnitt **Vorgänge** → **Lizenzierung** → **Lizenzen** des Hauptmenüs an die verwalteten Geräte bereitstellen.

- Verschieben Sie die Aktivierung der Anwendung



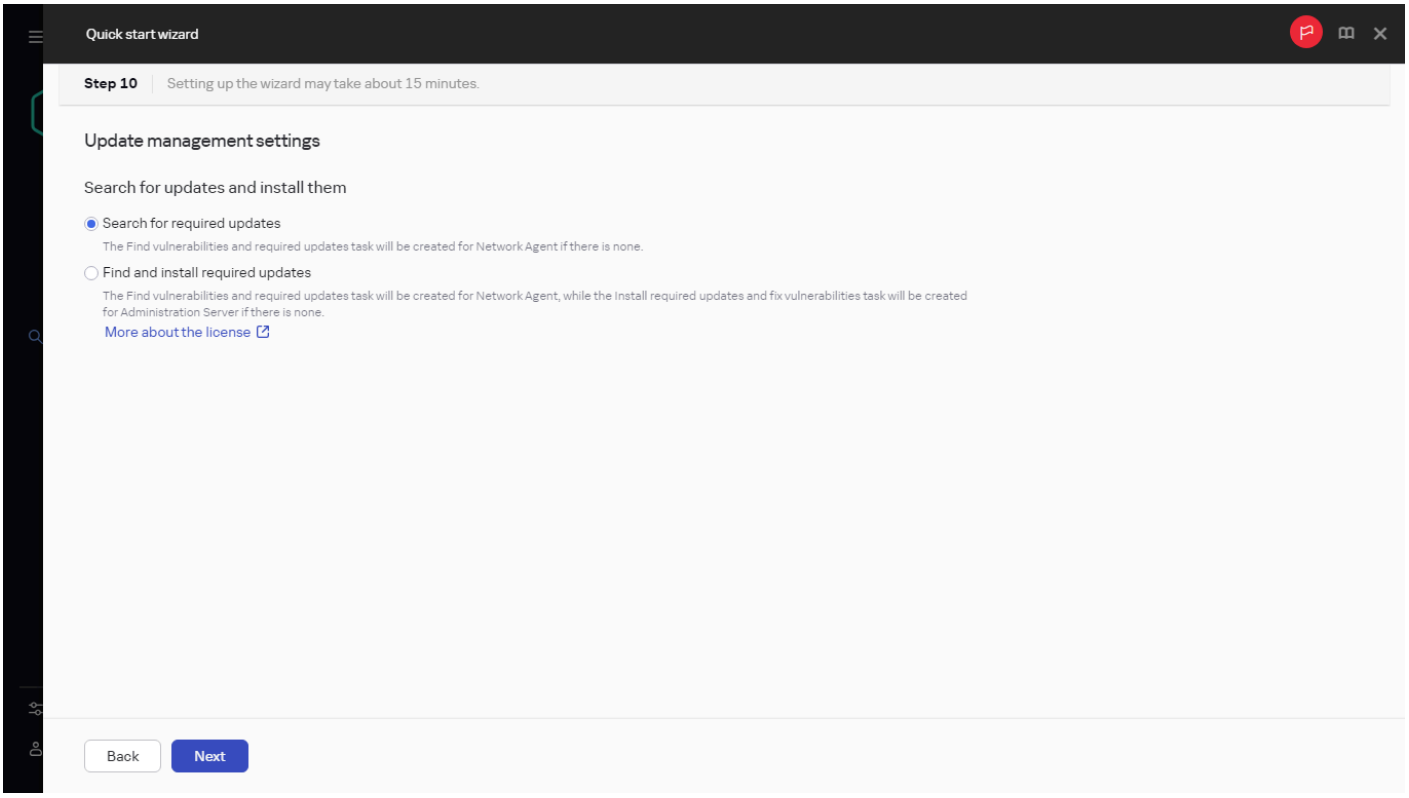
Auswählen der Methode zur Programmaktivierung

Wenn Sie die verschobene Aktivierung der Anwendung ausgewählt haben, können Sie den Lizenzschlüssel später jederzeit hinzufügen, indem Sie **Vorgänge** → **Lizenzierung** auswählen.

Wenn Sie mit Kaspersky Security Center aus einem gebührenpflichtigen AMI oder mit einem nutzungsbasierten, monatlich verrechneten SKU arbeiten, können Sie keine Schlüsseldateien angeben oder Aktivierungscodes eingeben.

Schritt 9. Einstellungen zur Verwaltung von Drittanbieter-Updates festlegen

Im Schnellstartassistenten wird der Schritt **Einstellungen für die Verwaltung von Updates** nicht angezeigt, wenn Sie keine Lizenz für das Schwachstellen- und Patch-Management besitzen oder wenn die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* bereits existiert.



Einstellungen zur Verwaltung von Drittanbieter-Updates

Wählen Sie für Updates von Drittanbieter-Programmen eine der folgenden Varianten aus:

- **Nach benötigten Updates suchen**

  Falls die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* noch nicht vorhanden ist, wird sie automatisch erstellt.

  Diese Option ist standardmäßig ausgewählt.

- **Erforderliche Updates suchen und installieren**

  Die Aufgaben *Suche nach Schwachstellen und erforderlichen Updates* und *Erforderliche Updates installieren und Schwachstellen schließen* werden automatisch erstellt, sofern sie noch nicht vorhanden sind.

  Diese Option ist nur im Rahmen der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Wählen Sie für die Updates aus Windows-Update die Option **Die in der Domänenrichtlinie angegeben Update-Quellen verwenden** aus.

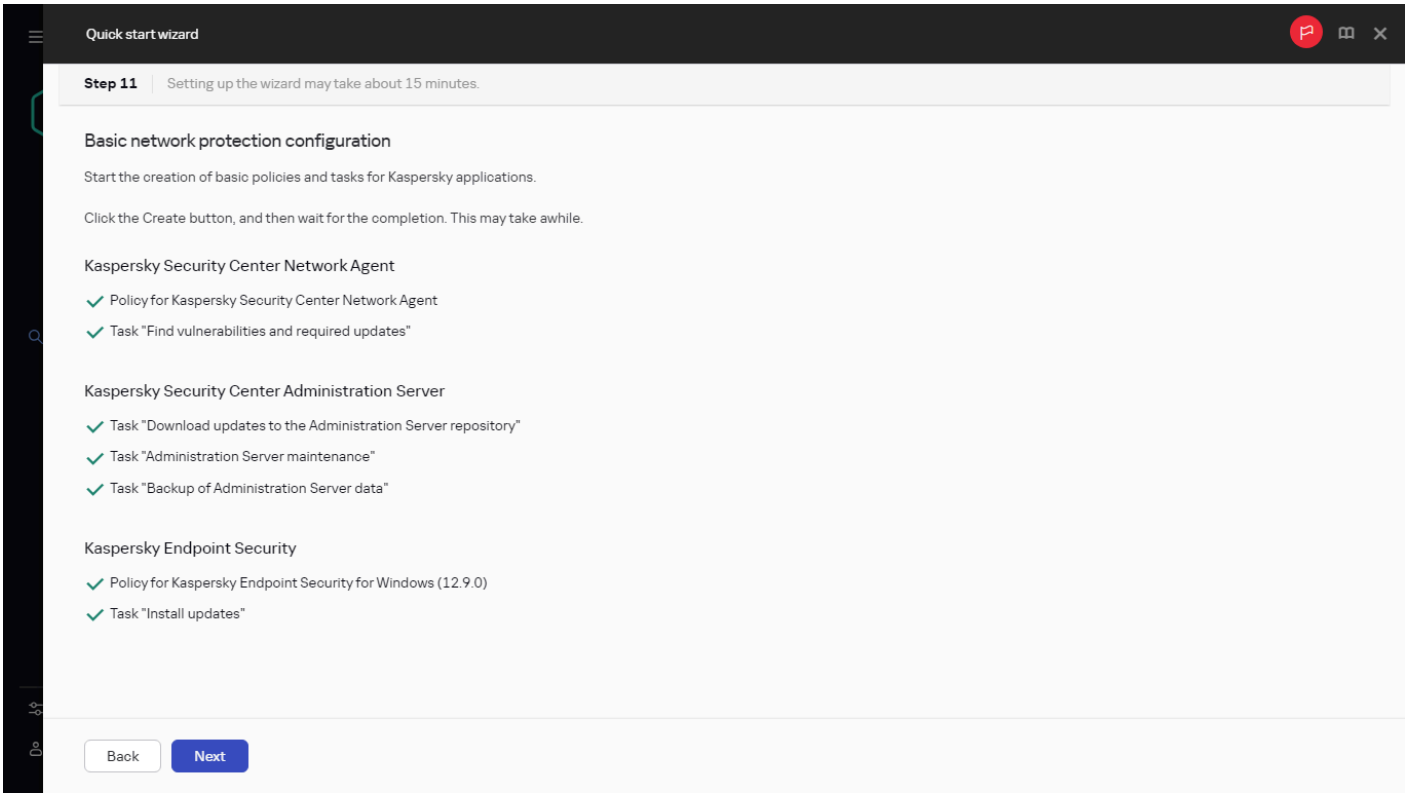
Die Client-Geräte laden Windows-Updates gemäß den Einstellungen Ihrer Domänenrichtlinie herunter. Die Richtlinie des Administrationsagenten wird automatisch erstellt, sofern sie noch nicht vorhanden ist.

Sie können die Aufgaben *Suche nach Schwachstellen und erforderlichen Updates* und *Erforderliche Updates installieren und Schwachstellen schließen* separat vom Schnellstartassistenten erstellen.

Schritt 10. Erstellen einer grundlegenden Konfiguration für Netzwerkschutz

Sie können die Liste mit Richtlinien und Aufgaben, die erstellt werden, überprüfen.

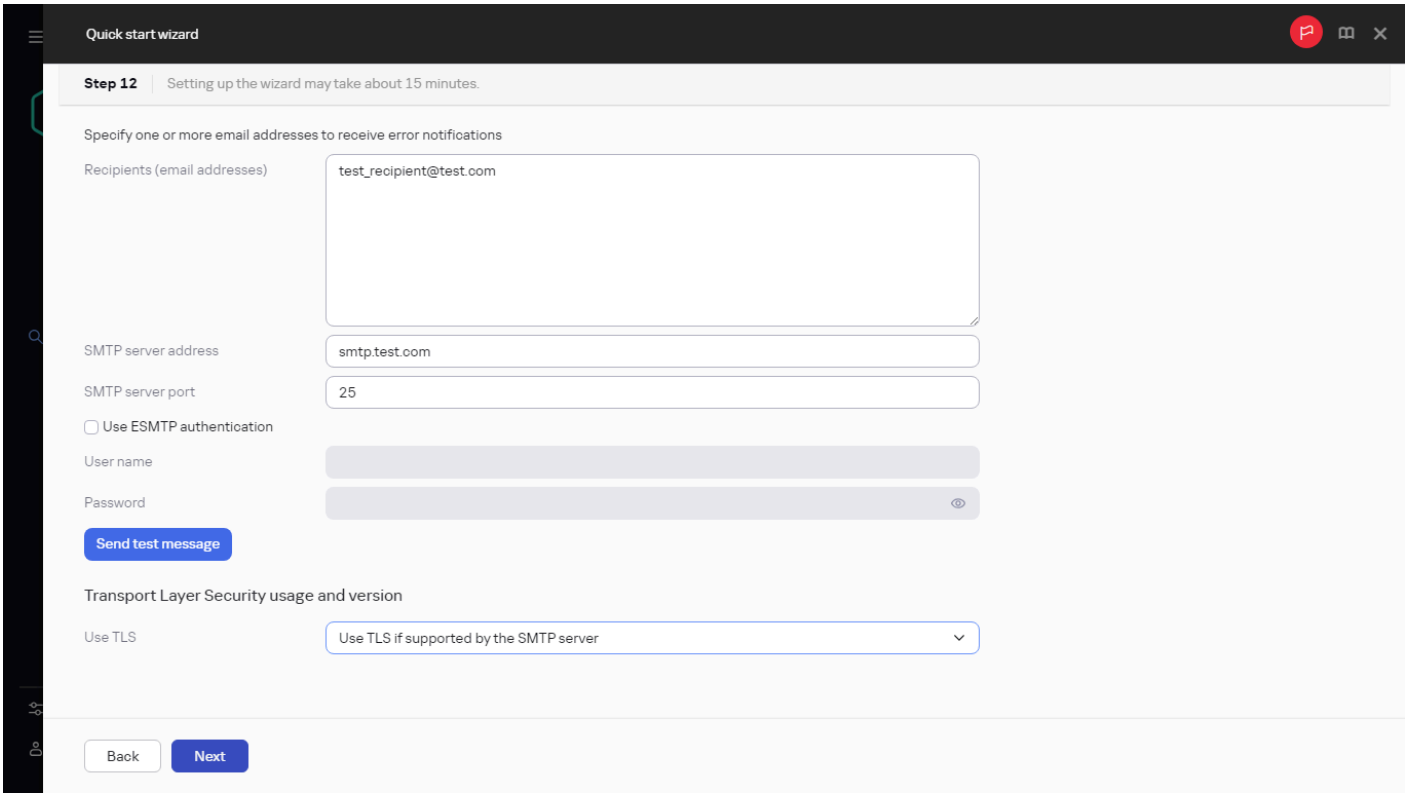
Bevor Sie zum nächsten Schritt des Assistenten wechseln können, müssen Sie warten, bis die Erstellung der Richtlinien und Aufgaben abgeschlossen ist.



Erstellen einer grundlegenden Konfiguration für Netzwerkschutz

Schritt 11. E-Mail-Benachrichtigungen konfigurieren

Passen Sie die Einstellungen für den Versand von Benachrichtigungen über Ereignisse an, die bei der Ausführung von Kaspersky-Anwendungen auf den Client-Geräten registriert werden. Diese Einstellungen werden in den Richtlinien für die Anwendungen als Standardwerte verwendet.



Konfigurieren von E-Mail-Benachrichtigungen

Folgende Einstellungen für den Versand von Benachrichtigungen über auftretende Ereignisse der Kaspersky-Anwendungen können angepasst werden:

- **Empfänger (E-Mail-Adressen)**

  E-Mail-Adressen des Nutzers, an welche die Anwendung Benachrichtigungen versenden soll. Sie können eine oder mehrere Adressen angeben. Geben Sie mehrere Adressen durch Semikolon getrennt an.

- **Adresse des SMTP-Servers**

  Adresse oder Adressen der Mail-Server Ihres Unternehmens.

  Geben Sie mehrere Adressen durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

  - IPv4- oder IPv6-Adresse
  - DNS-Name des SMTP-Servers

- **Port des SMTP-Servers**

  Kommunikationsportnummer des SMTP-Servers Wenn Sie mehrere SMTP-Server verwenden, wird die Verbindung zu diesen über den angegebenen Kommunikationsport hergestellt. Standardmäßig wird Portnummer 25 verwendet.

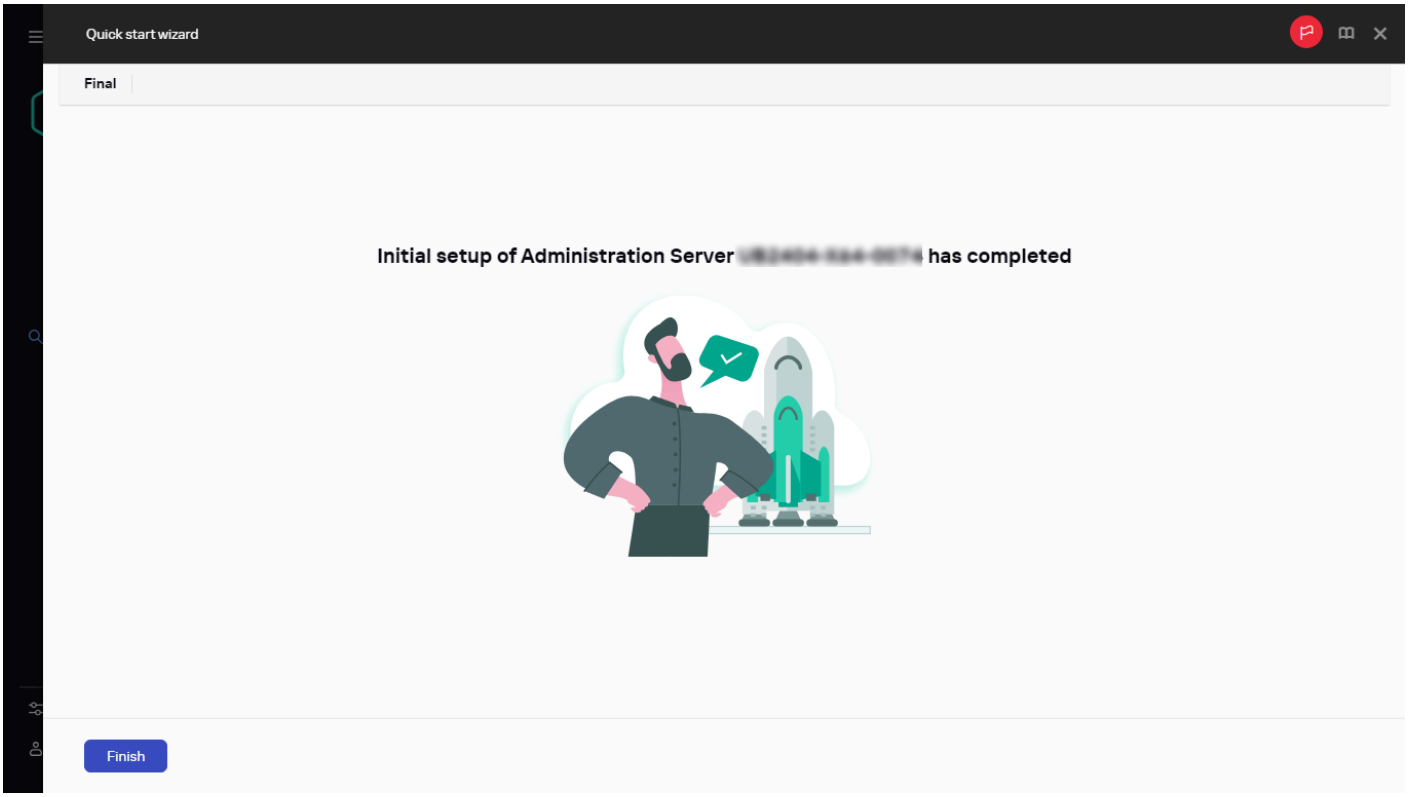
- **ESMTP-Authentifizierung verwenden**

  Aktivierung der Unterstützung von ESMTP-Authentifizierung. Nach der Aktivierung des Kontrollkästchens in den Feldern **Benutzername** und **Kennwort** können die Einstellungen für ESMTP-Authentifizierung angeben werden. Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

Sie können die festgelegten Versandeinstellungen der E-Mail-Benachrichtigungen mithilfe der Schaltfläche **Testnachricht senden** prüfen.

Schritt 12. Schnellstartassistent abschließen

Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen.



Abschließender Schritt des Schnellstartassistenten

Nachdem Sie den Schnellstartassistenten abgeschlossen haben, können Sie den Assistenten für die Bereitstellung des Schutzes ausführen um Anti-Virus-Anwendungen oder den Administrationsagenten automatisch auf Geräten in Ihrem Netzwerk zu installieren.

Assistent für die Bereitstellung des Schutzes

Um Kaspersky-Anwendungen zu installieren, können Sie den Assistenten für die Bereitstellung des Schutzes verwenden. Der Assistent für die Bereitstellung des Schutzes ermöglicht die Remote-Installation von Anwendungen entweder mit zuvor speziell erstellten Installationspaketen oder direkt aus den Programmpaketen.

Der Assistent für die Bereitstellung des Schutzes führt die folgenden Aktionen aus:

- Herunterladen eines Installationspaket für die Anwendung (falls es zuvor nicht erstellt wurde). Das Installationspaket befindet sich unter **Software-Verwaltung → Installationspakete**. Dieses Installationspaket kann zur weiteren Installation des Programms herangezogen werden.

- Erstellen und starten eine Aufgabe zur Remote-Installation für eine Reihe von Geräten oder für eine Administrationsgruppe. Die soeben erstellte Aufgabe zur Remote-Installation wird in dem Abschnitt **Aufgaben** gespeichert. Sie können diese Aufgabe später manuell starten. Der Aufgabentyp ist **Remote-Installation einer Anwendung**.

Wenn Sie den Administrationsagenten auf Geräten mit dem Betriebssystem SUSE Linux Enterprise Server 15 installieren möchten, sollten Sie zunächst das Paket insserv-compat installieren, um den Administrationsagenten konfigurieren.

Schritt 1. Assistent für die Bereitstellung des Schutzes starten

Sie können den Assistenten für die Bereitstellung des Schutzes jederzeit manuell starten.

So starten Sie den Assistenten für die Bereitstellung des Schutzes manuell:

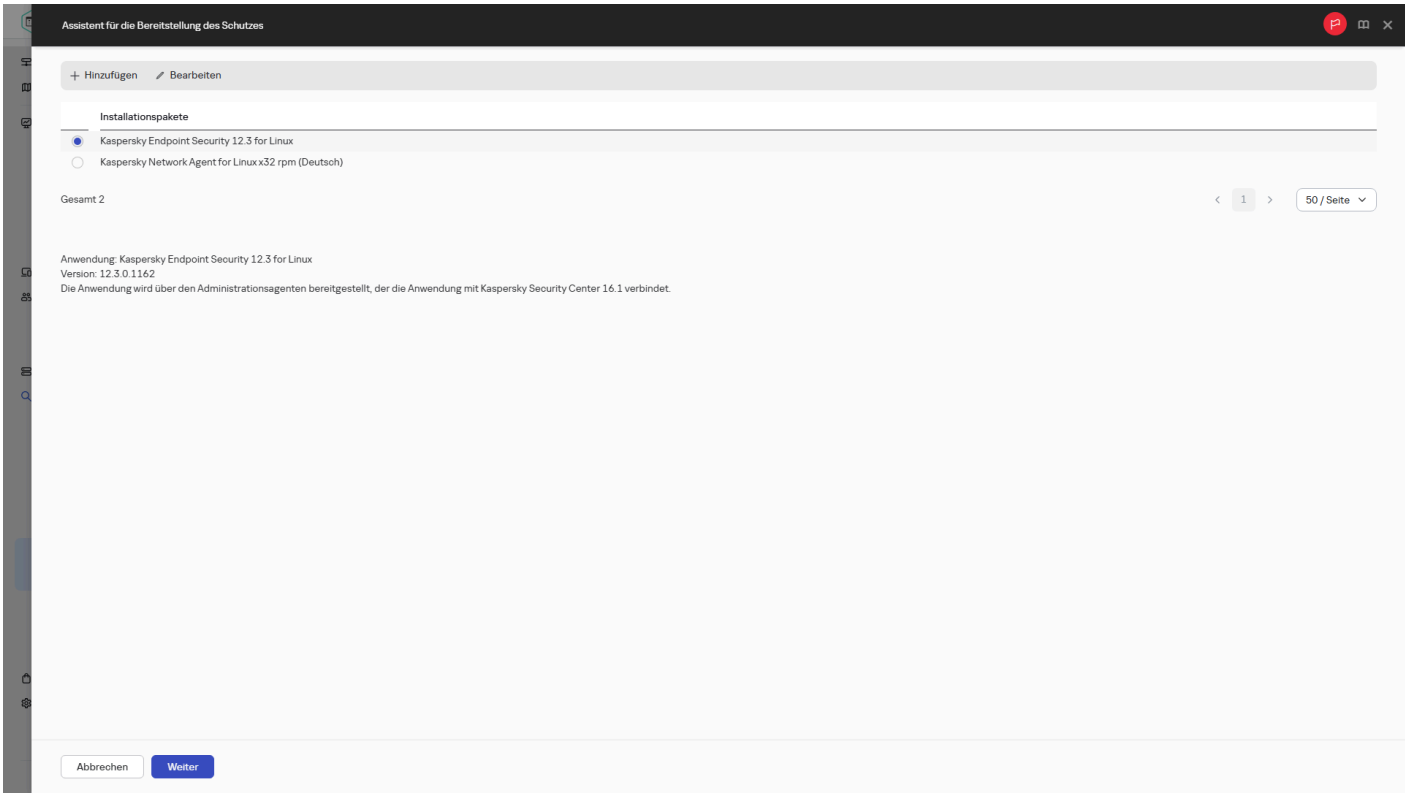
Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Assistent für die Bereitstellung des Schutzes**.

Der Assistent für die Bereitstellung des Schutzes wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

Schritt 2. Installationspaket auswählen

Wählen Sie das Installationspaket der Anwendung, das Sie installieren möchten.

Wenn das Installationspaket der gewünschten Anwendung nicht aufgeführt ist, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie anschließend die Anwendung aus der Liste aus.



Das Installationspaket auswählen

Schritt 3. Verteilungsmethode der Schlüsseldatei oder des Aktivierungscodes auswählen

Wählen Sie eine Methode zur Verteilung einer Schlüsseldatei oder eines Aktivierungscodes aus:

- **Lizenzschlüssel nicht zum Installationspaket hinzufügen**

  Der Schlüssel wird automatisch auf alle Geräte verteilt, mit denen er kompatibel ist:

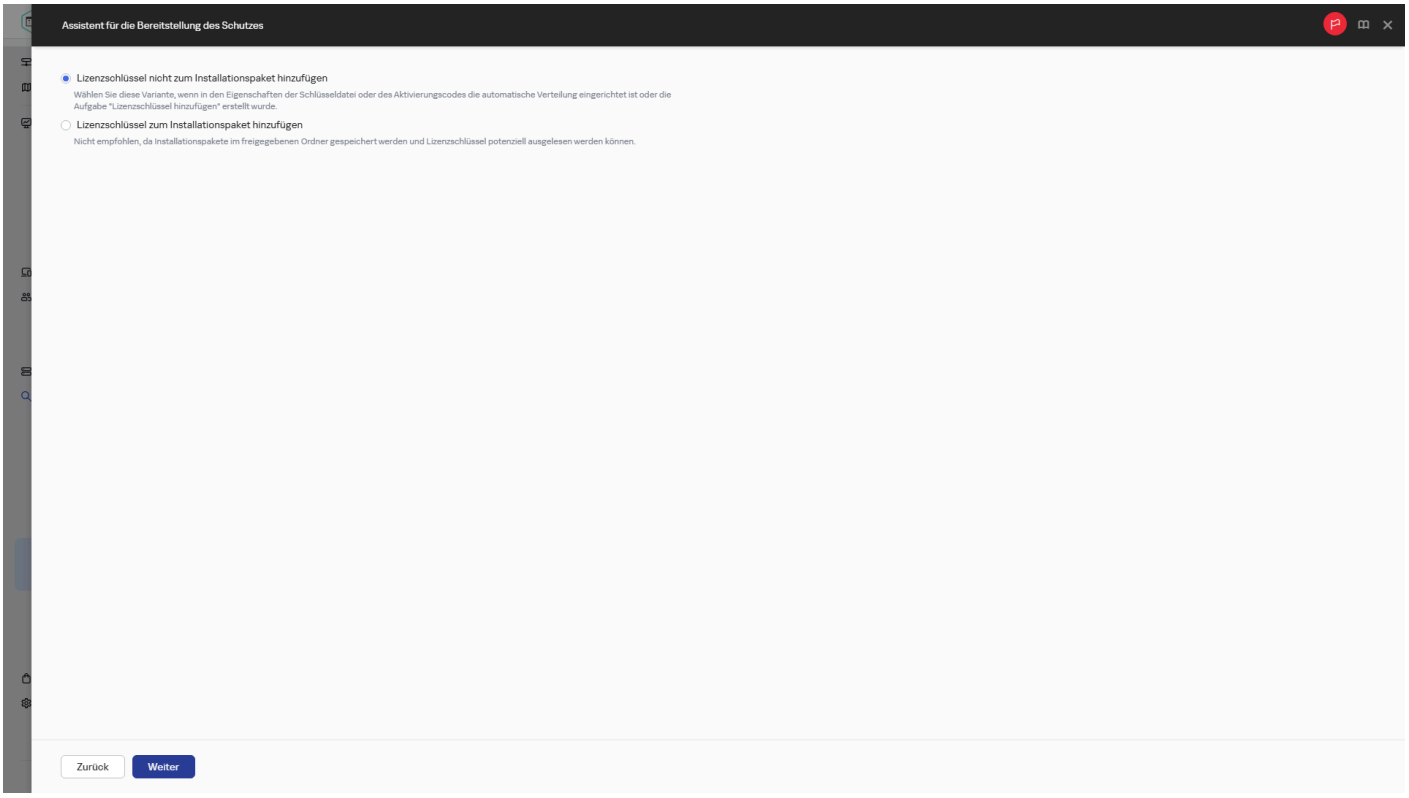
  - Wenn in den Eigenschaften des Schlüssel die automatische Verteilung aktiviert ist.
  - Wenn die Aufgabe **Schlüssel hinzufügen** erstellt wurde.

- **Lizenzschlüssel zum Installationspaket hinzufügen**

  Der Schlüssel wird gemeinsam mit dem Installationspaket an Geräte verteilt.

  > Es wird nicht empfohlen, den Schlüssel auf diese Art zu verteilen, da die Datenverwaltung der Installationspakete über allgemeinen Lesezugriff verfügt.

Wenn eine Schlüsseldatei oder ein Aktivierungscode bereits zum Installationspaket gehören, wird dieses Fenster angezeigt; enthält dann aber nur Informationen über den Lizenzschlüssel.

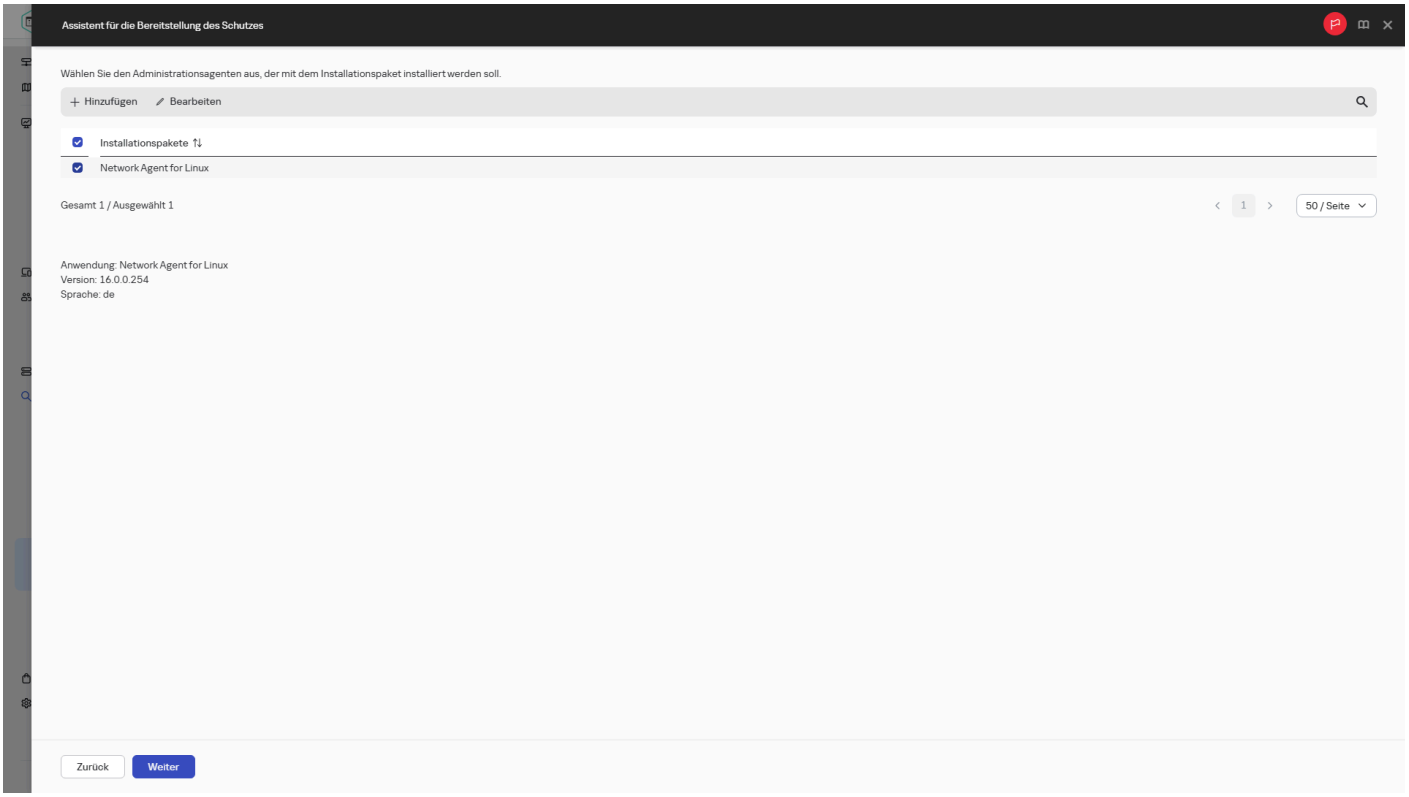


Auswählen der Verteilungsmethode der Schlüsseldatei oder des Aktivierungscodes

Schritt 4. Auswählen der Version des Administrationsagenten

Wenn Sie das Installationspaket einer anderen Anwendung ausgewählt haben (nicht den Administrationsagenten), müssen Sie auch den Administrationsagenten installieren, da dieser die Anwendung mit dem Kaspersky Security Center Administrationsserver verbindet.

Wählen Sie die aktuellste Version des Administrationsagenten aus.



Auswahl der Version des Administrationsagenten

Schritt 5. Auswählen der Geräte

Geben Sie eine Liste mit Geräte an, auf denen die Anwendung installiert werden soll:

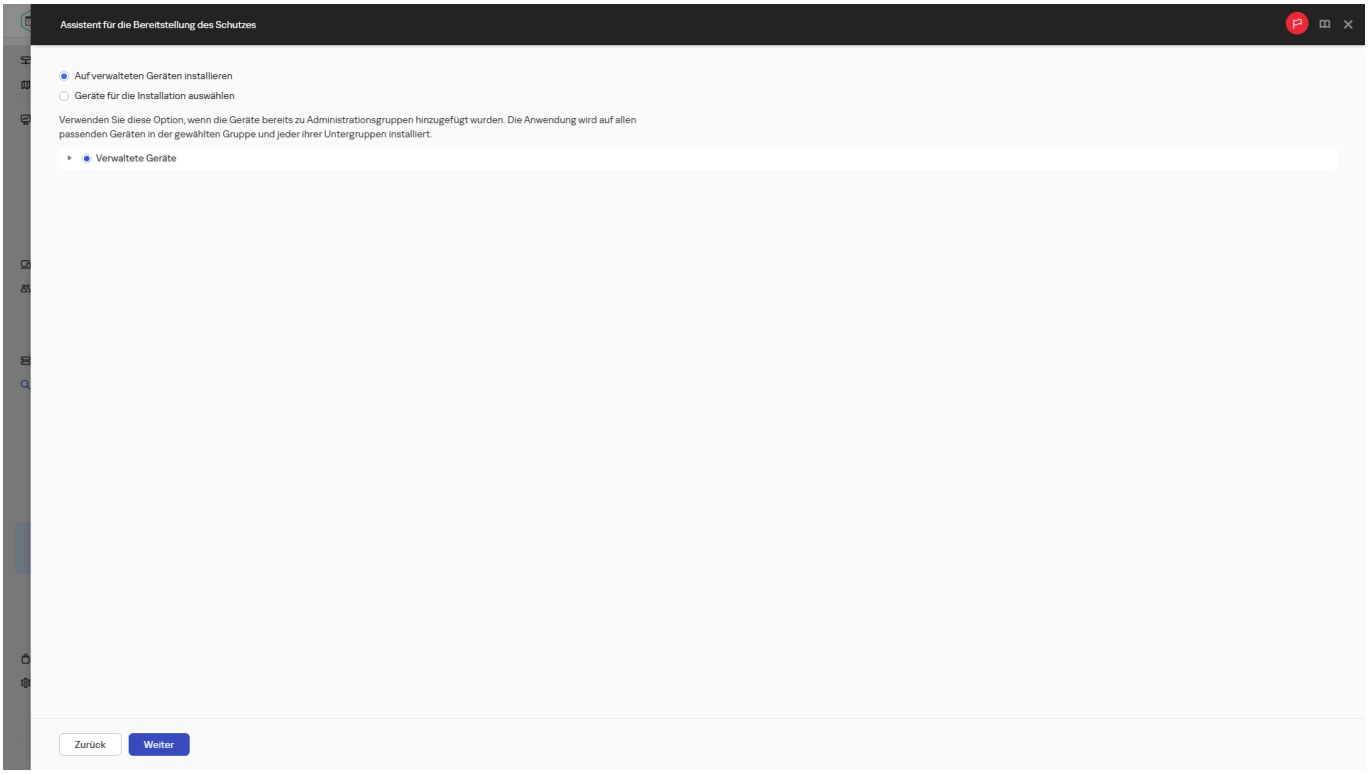
- **Auf verwalteten Geräten installieren**

  Bei Auswahl dieser Option wird die Aufgabe zur Remote-Installation eines Programms für eine Gerätegruppe erstellt.

- **Geräte für die Installation auswählen**

  Die Aufgabe wird Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.



Angabe einer Liste mit Geräten, auf denen die Anwendung installiert wird

Schritt 6. Festlegen der Einstellungen für die Aufgabe zur Remote-Installation

Passen Sie auf der Seite **Einstellungen für die Aufgabe zur Remote-Installation** die Einstellungen für die Remote-Installation einer Anwendung.

Wählen Sie in der Einstellungsgruppe **Download des Installationspakets erzwingen** die Methode der Übertragung der zur Anwendungsinstallation erforderlichen Dateien auf die Client-Geräte aus:

- **Unter Nutzung des Administrationsagenten**

  Wenn die Option aktiviert ist, werden die Installationspakete von dem auf den Client-Geräten installierten Administrationsagenten zugestellt.

  Wenn diese Option deaktiviert ist, werden Installationspakete mithilfe der Betriebssystems-Tools der Client-Geräte ausgeliefert.

  Es wird empfohlen, die Option zu aktivieren, wenn die Aufgabe für Geräte mit installierten Administrationsagenten vorgesehen ist.

  Diese Option ist standardmäßig aktiviert.

- **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**

  Wenn diese Option aktiviert ist, werden Installationspakete mithilfe der Tools von den Betriebssystemen durch Verteilungspunkte auf die Geräte übertragen. Diese Variante ist wählbar, wenn sich im Netzwerk mindestens ein Verteilungspunkt befindet.

  Ist die Option **Mithilfe des Administrationsagenten** aktiviert, werden die Dateien nur dann mit den Betriebssystem-Tools zugestellt, wenn die Funktionen des Administrationsagenten nicht verwendet werden können.

Standardmäßig ist diese Option für die Aufgaben von Remote-Installationen aktiviert, die auf einem virtuellen Administrationsserver erstellt wurden.

Die einzige Möglichkeit, eine Windows-Anwendung (einschließlich Administrationsagent für Windows) auf einem Gerät zu installieren, auf dem kein Administrationsagent installiert ist, besteht in der Verwendung eines Windows-basierten Verteilungspunkts. Wenn Sie daher eine Windows-Anwendung installieren wollen:

- Wählen Sie diese Option.
- Stellen Sie sicher, dass den Ziel-Client-Geräten ein Verteilungspunkt zugewiesen ist.
- Stellen Sie sicher, dass der Verteilungspunkt Windows-basiert ist.

- **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**

  Wenn diese Option aktiviert ist, werden die Dateien durch den Administrationsserver mittels Betriebssystem-Tools der Client-Gerät auf die Client-Geräte übertragen. Diese Option kann aktiviert werden, wenn auf dem Client-Gerät kein Administrationsagent installiert ist, das Client-Gerät sich aber im selben Netzwerk wie der Administrationsserver befindet.

  Diese Option ist standardmäßig aktiviert.

Passen Sie die erweiterte Einstellung an:

- **Anwendung nicht neu installieren, wenn sie bereits installiert ist**

  Wenn diese Option aktiviert ist, wird die ausgewählte Anwendung nicht neu installiert, wenn sie bereits auf dem Client-Gerät installiert ist.

  Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Anwendung in jedem Fall installiert.

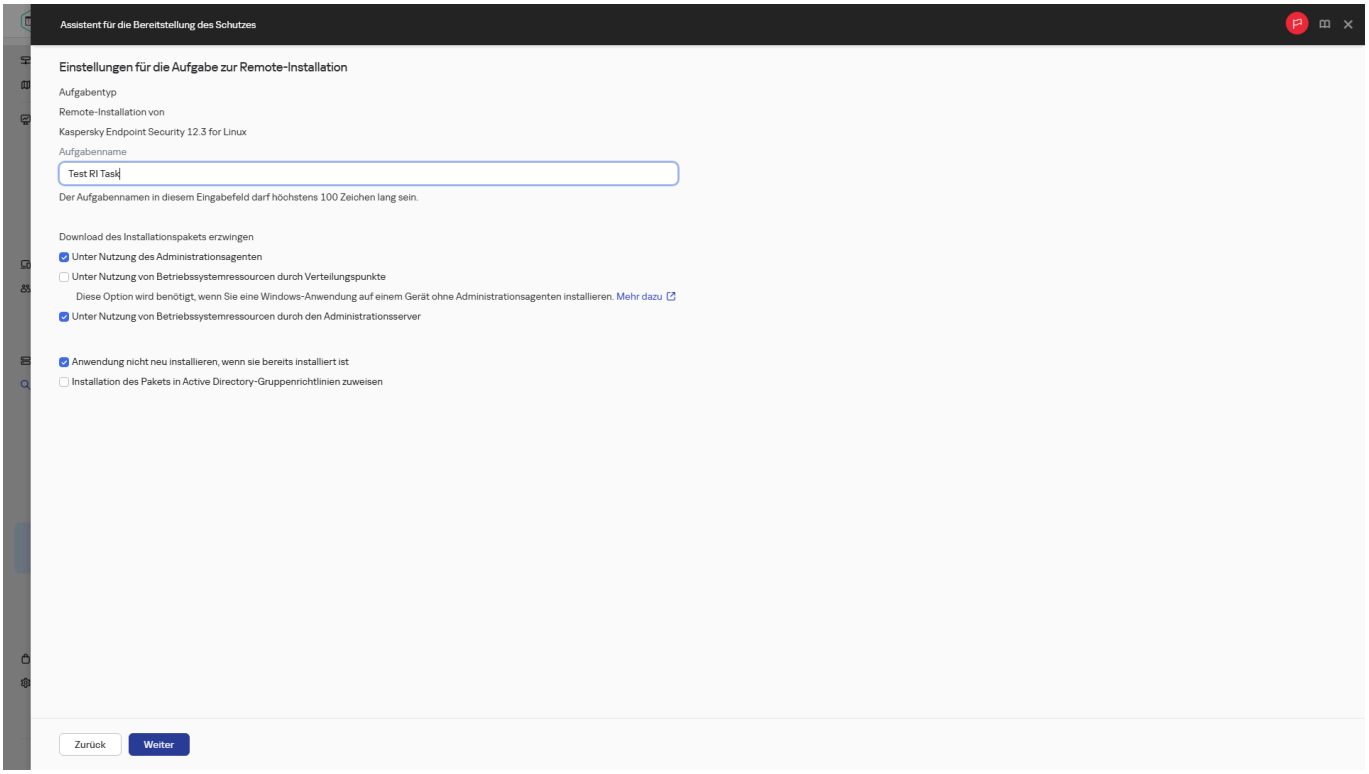
  Diese Option ist standardmäßig aktiviert.

- **Installation des Pakets in Active Directory-Gruppenrichtlinien zuweisen**

  Wenn diese Option aktiviert ist, wird das Installationspaket mithilfe von Richtlinien des Active Directory installiert.

  Die Option ist verfügbar, wenn ein Installationspaket des Administrationsagenten ausgewählt ist.

Diese Option ist standardmäßig deaktiviert.



Angabe der Einstellungen für die Aufgabe zur Remote-Installation

Schritt 7. Verwaltung des Neustarts

Geben Sie an, welche Aktion ausgeführt werden soll, wenn das Betriebssystem bei der Installation des Programms neu gestartet werden muss:

- **Gerät nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

- **Gerät neu starten**

  Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

Diese Option ist standardmäßig ausgewählt.

- **Aufforderung wiederholen alle (Min.)**

  Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

  Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten nach (Min.)**

  Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

  Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

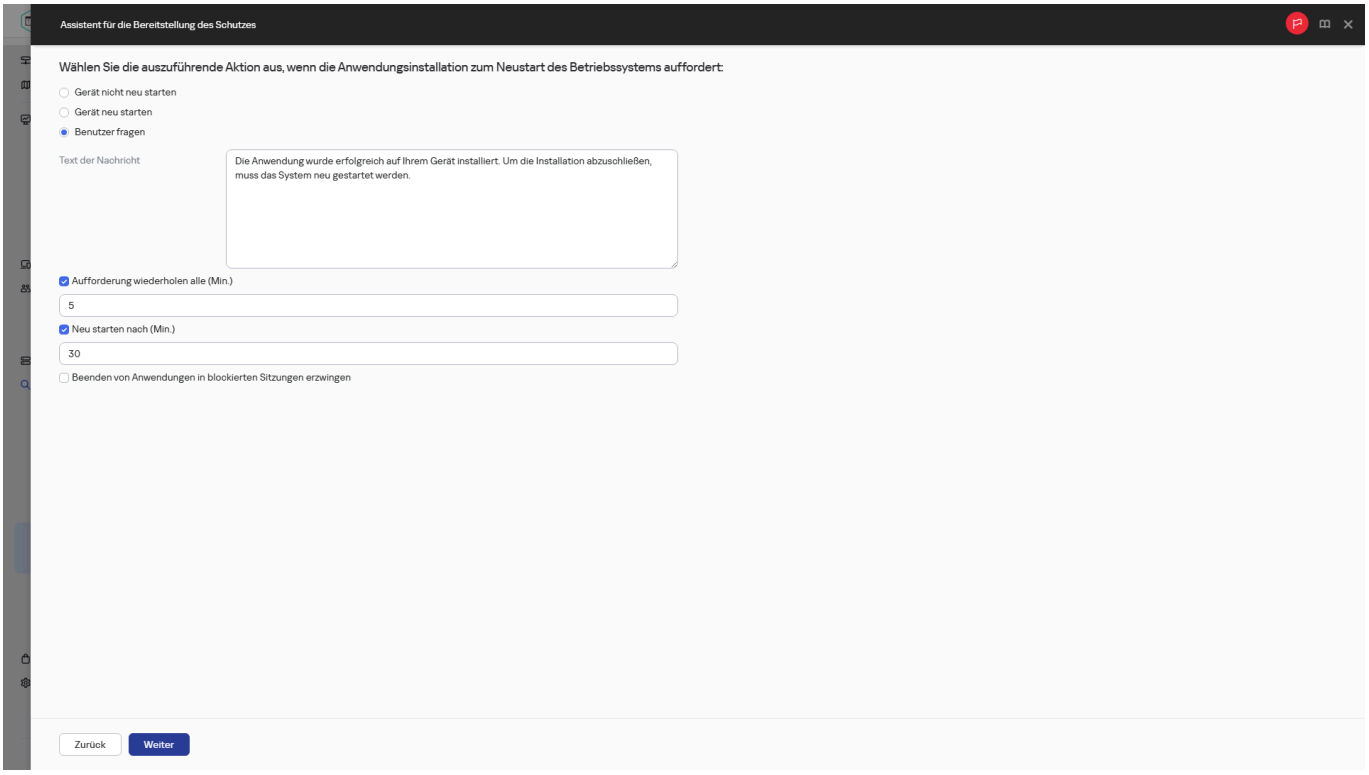
- **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.



Auswahl der Neustart-Option des Betriebssystems

Schritt 8. Deinstallieren inkompatibler Programme vor der Installation

Dieser Schritt ist nur dann verfügbar, wenn die zu verteilende Anwendung bekanntlich mit anderen Anwendungen inkompatibel ist.

Wählen Sie diese Option, wenn Sie möchten, dass Kaspersky Security Center Linux automatisch Anwendungen deinstalliert, die mit der zu verteilenden Anwendung inkompatibel sind.

Die Liste der inkompatiblen Anwendungen wird ebenfalls angezeigt.

Wenn Sie diese Option nicht auswählen, wird die Anwendung nur auf Geräten installiert, die keine inkompatiblen Anwendungen aufweisen.

Schritt 9. Verschieben von Geräten in die Gruppe "Verwaltete Geräte"

Geben Sie an, ob die Geräte nach Abschluss der Installation des Administrationsagenten in die Administrationsgruppe verschoben werden müssen.

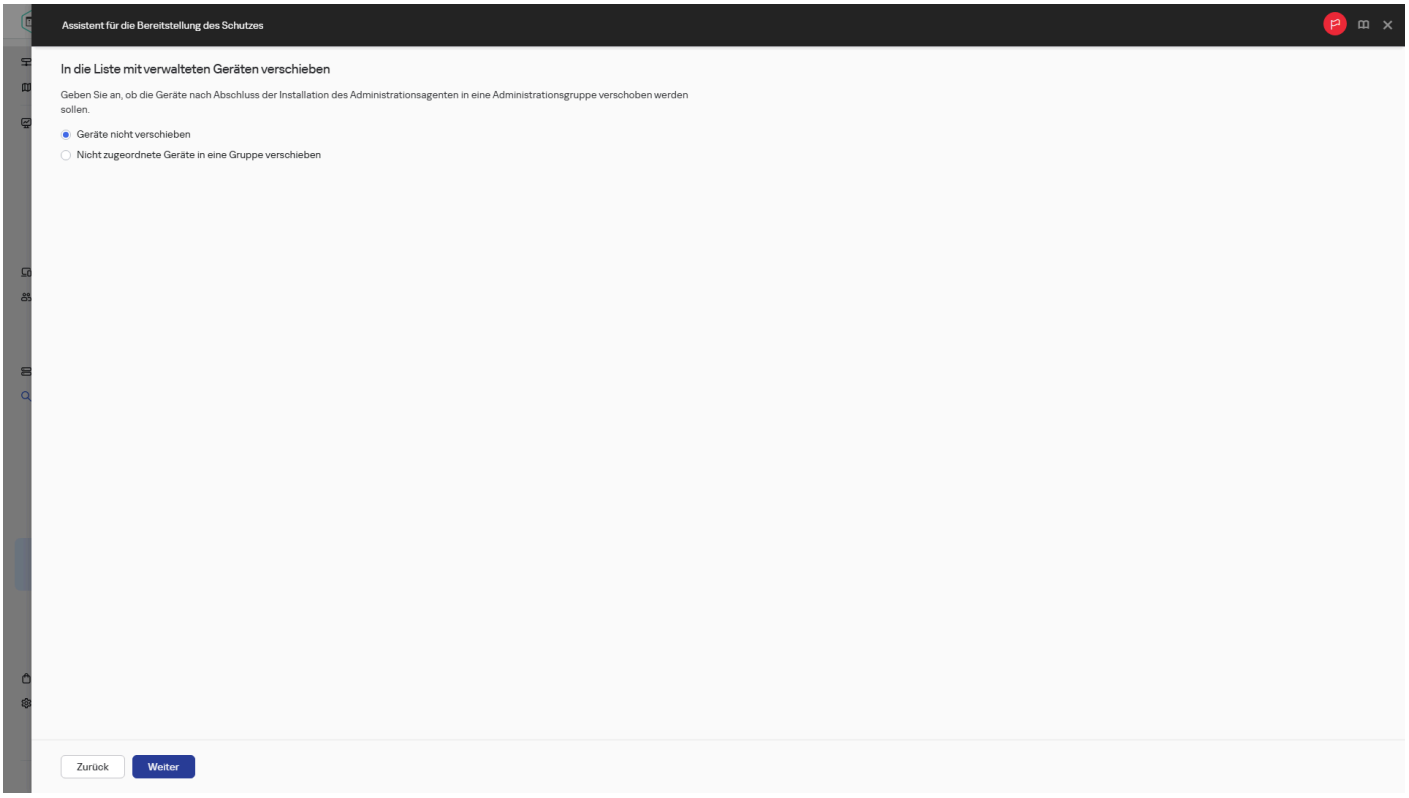
- **Geräte nicht verschieben**

  Die Geräte bleiben in den Gruppen, in denen sie sich gerade befinden. Die Geräte, die keiner Gruppe zugeordnet wurden, bleiben nicht zugeordnet.

- **Nicht zugeordnete Geräte in eine Gruppe verschieben**

  Die Geräte werden in die ausgewählte Administrationsgruppe verschoben.

Die Variante **Geräte nicht verschieben** ist standardmäßig festgelegt. Aus Sicherheitsgründen sollten Sie die Geräte manuell verschieben.



Auswahl einer Option zum Verschieben von Geräten in eine Administrationsgruppe

Schritt 10. Auswählen von Benutzerkonten für den Zugriff auf Geräten

Bei Bedarf können Sie Benutzerkonten hinzufügen, die für den Start der Aufgabe zur Remote-Installation verwendet werden sollen:

- **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**

  Wenn diese Variante ausgewählt ist, muss das Benutzerkonto nicht angegeben werden, unter dem das Installationsprogramm der Anwendung gestartet werden soll. Die Aufgabe wird unter dem Konto gestartet, unter dem der Dienst des Administrationsservers läuft.

  Wenn der Administrationsagent nicht auf den Client-Geräten installiert ist, steht diese Option nicht zur Verfügung.

- **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)**

  Wählen Sie diese Option, wenn auf den Geräten, denen Sie die Aufgabe zur Remote-Installation zuweisen, der Administrationsagent nicht installiert ist. In diesem Fall können Sie ein Benutzerkonto oder ein SSH-Zertifikat angeben, um die Anwendung zu installieren.

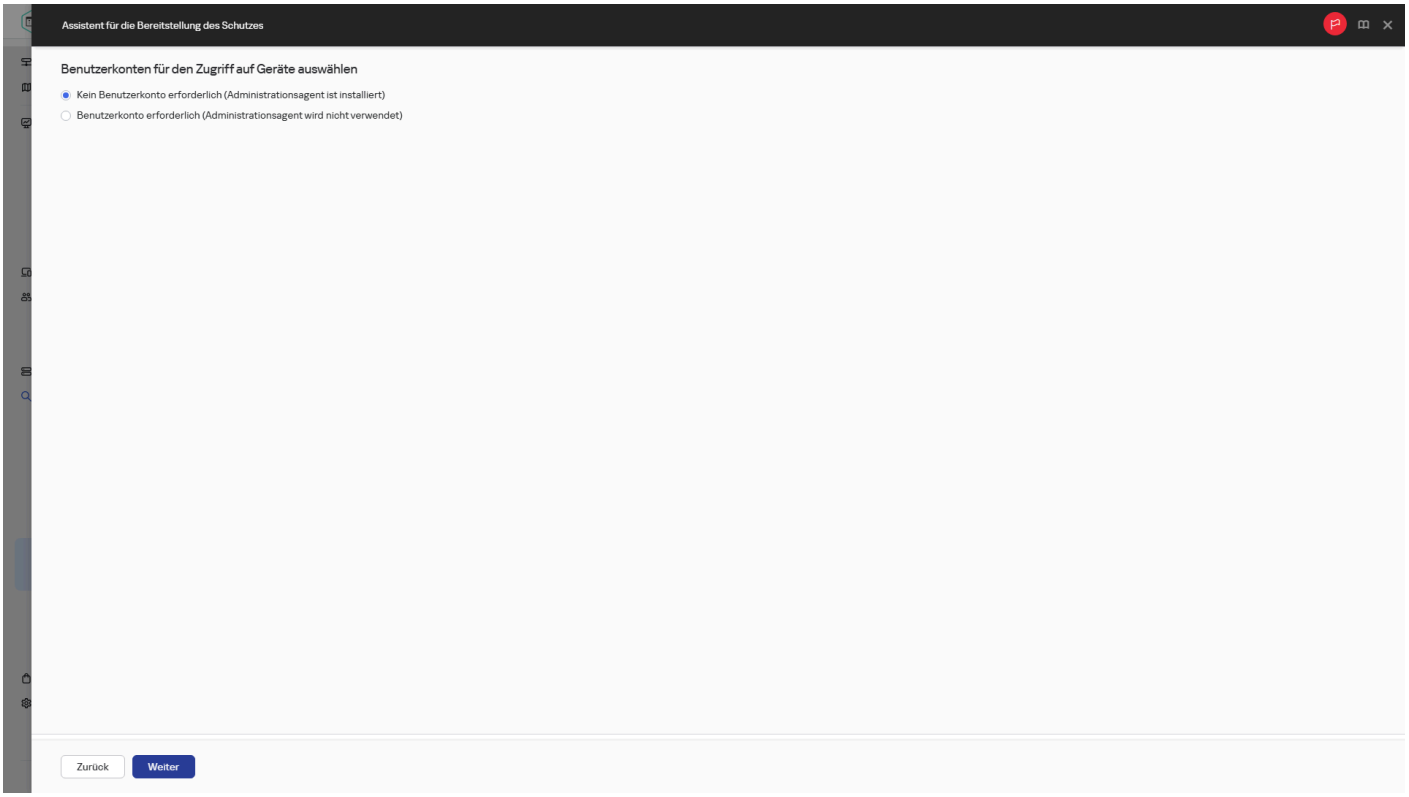
  - **Lokales Konto oder Domänenkonto**. Wenn Sie diese Variante auswählen, können Sie das Benutzerkonto angeben, unter dem das Installationsprogramm gestartet werden soll. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Lokales Konto oder Domänenkonto** aus, und geben Sie anschließend die Anmeldeinformationen des Benutzerkontos an.

    Sie können mehrere Benutzerkonten angeben, wenn beispielsweise kein Benutzerkonto existiert, dass über die erforderlichen Rechte auf allen Geräten verfügt, für welche die Aufgabe bestimmt wurde. In diesem Fall werden für den Start der Aufgabe alle hinzugefügten Konten nacheinander von oben nach unten angewandt.

- **SSH-Zertifikat**. Wenn Sie eine Anwendung auf einem Linux-basierten Client-Gerät installieren möchten, können Sie anstelle eines Benutzerkontos ein SSH-Zertifikat angeben. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **SSH-Zertifikat** aus, und geben Sie anschließend den privaten und den öffentlichen Schlüssel des Zertifikats an.

  Um einen privaten Schlüssel zu generieren, können Sie das Tool "ssh-keygen" verwenden. Beachten Sie, dass die Kaspersky Security Center Linux das pem-Format für private Schlüssel verwendet, das Tool "ssh-keygen" jedoch standardmäßig SSH-Schlüssel im OpenSSH-Format generiert. Das OpenSSH-Format wird von Kaspersky Security Center Linux nicht unterstützt. Um einen privaten Schlüssel im unterstützten pem-Format zu erstellen, fügen Sie die dem Befehl "ssh-keygen" den Parameter "-m PEM" hinzu. Beispielsweise:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<Benutzer-E-Mail>"
  ```



Auswahl von Benutzerkonten für den Zugriff auf Geräte

Schritt 11. Installation starten

Dies ist der abschließende Schritt des Assistenten. In diesem Schritt wurde die **Aufgabe zur Remote-Installation** erfolgreich erstellt und konfiguriert.

Die Variante **Aufgabe nach Abschluss des Assistenten starten** ist standardmäßig nicht ausgewählt. Wenn Sie diese Option auswählen, startet die **Aufgabe zur Remote-Installation** sofort nach Abschluss des Assistenten. Wenn Sie diese Option nicht auswählen, startet die **Aufgabe zur Remote-Installation** nicht. Sie können diese Aufgabe später manuell starten.

Klicken Sie auf **OK**, um den letzten Schritt des Assistenten für die Bereitstellung des Schutzes abzuschließen.

Kaspersky Security Center Linux aktualisieren

Sie können Version 16.3 des Administrationsservers auf einem Gerät installieren, auf dem eine ältere Version des Administrationsservers installiert ist (ab Version 13). Beim Aktualisieren auf die Version 16.3 bleiben alle Daten und Einstellungen der vorherigen Version des Administrationsservers erhalten.

Erforderliche Vorrausetzungen

- Erstellen Sie eine Backup-Kopie der Daten des Administrationsservers vor Beginn des Upgrades.
- Beim Upgrade des Administrationsservers von Version 16 oder früher auf Version 16.1 oder später wird die Zwei-Faktor-Authentifizierung aktiviert. Weitere Informationen finden Sie unter Über die zweistufige Überprüfung für ein Konto.

  Um sicherzustellen, dass Benutzer Bei der Webkonsole anmelden mit ihren bestehenden Konten unter Verwendung konfigurierter geheimer Schlüssel für die Zwei-Faktor-Authentifizierung, und dass OpenAPI-Automatisierungsskripte Um nach dem Upgrade weiterarbeiten zu können, müssen Sie die folgenden Schritte ausführen:

  - Zwei-Faktor-Authentifizierung für alle Benutzer aktivieren
  - Administratoren müssen die Zwei-Faktor-Authentifizierung für ihre eigenen Konten konfigurieren
  - Die erforderlichen Konten von der Zwei-Faktor-Authentifizierung ausschließen

    Fügen Sie bei Bedarf Integrationskonten, die zum Ausführen von Skripten über OpenAPI verwendet werden, zur Ausschlussliste hinzu.
- Stellen Sie sicher, dass Sie die Versionen des Betriebssystems und des DBMS verwenden, die vom Administrationsserver in Version 16.3 unterstützt. Bei Bedarf können Sie den Administrationsserver auf ein anderes Gerät mit aktuelleren Versionen des Betriebssystems und des DBMS verschieben.
- Wenn Sie den Administrationsserver Version 15.4 oder früher auf Version 16 oder später aktualisieren, erstellen Sie auf dem DBMS-Server eine Datenbank für IAM. Der Name der Datenbank muss sich von dem Namen der Datenbank unterscheiden, die Sie für die Verwendung mit Kaspersky Security Center Linux installiert haben.

  - Für PostgreSQL führen Sie den folgenden Befehl aus:

    ```
    sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <iam_db_name>;"
    ```

  - Für MariaDB führen Sie den folgenden Befehl aus:

    ```
    sudo mysql -u root -p -e "CREATE DATABASE <iam_db_name>;"
    ```
- Wenn Sie den Administrationsserver Version 15.4 oder früher auf Version 16 oder später aktualisieren, erstellen Sie die Antwortdatei mit neuen Parametern für IAM. Eine Liste der erforderlichen Parameter finden Sie in folgendem Artikel: Installation von Kaspersky Security Center Linux im Silent-Modus. Fügen Sie die Umgebungsvariable `KLAUTOANSWERS` hinzu und geben Sie für ihren Wert den Pfad zur Antwortdatei an.
- Machen Sie den Port verfügbar, der vom Prozess "kliam" für die Authentifikation des OpenID Connect-Protokolls verwendet wird. Standardmäßig ist dies 4444. Weite Informationen finden Sie in dem Artikel Installationsparameter für Kaspersky Security Center Web Console unter dem Parameter `trusted`.

Schritte

1 Aktualisierung des Administrationsservers

Für das Upgrade einer Version des Administrationsservers gibt es die folgenden Methoden:

- Verwendung der Installationsdatei für Kaspersky Security Center Linux
- Durch Anlegen eines Daten-Backups des Administrationsservers, Installation einer neuen Version des Administrationsservers und Wiederherstellung der Administrationsserver-Daten aus dem Backup

> Während des Upgrades ist unbedingt darauf zu achten, dass keine gemeinsame Nutzung des DBMS durch den Administrationsserver und einer anderen Anwendung stattfindet.

Wenn Ihr Netzwerk mehrere Administrationsserver umfasst, müssen Sie jeden Server manuell aktualisieren. Ein zentralisiertes Upgrade wird von Kaspersky Security Center Linux nicht unterstützt.

2 Ausführen des Skripts „postinstall.pl“ (optionaler Schritt)

Wenn die Antwortdatei keine IAM-Parameter enthält oder nicht vorhanden ist, wird während des Upgrades im Terminal eine Meldung angezeigt, die Sie auffordert, das Skript "postinstall.pl" auszuführen.

Führen Sie in diesem Schritt des Szenarios die folgenden Aktionen aus:

1. Erstellen Sie im Betriebssystem des Administrationsservers das nicht privilegierte Benutzerkonto "ksciam", das Mitglied der Gruppe "kladmins" sein muss:

   ```
   adduser ksciam
   gpasswd -a ksciam kladmins
   usermod -g kladmins ksciam
   ```

2. Führen Sie unter einem Benutzerkonto mit Root-Berechtigung das Skript /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl aus, um den Administrationsserver nach dem Upgrade zu konfigurieren. Geben Sie nach der entsprechenden Aufforderung die folgenden Einstellungen ein:

   1. Geben Sie den FQDN des IAM-Servers ein. Sie müssen den DNS-Namen des Administrationsservers verwenden, der bei der Installation von Kaspersky Security Center Linux angegeben wurde.
   2. Geben Sie den Namen des Kontos ein, um den IAM-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto "ksciam" verwendet.
   3. Wählen Sie das DBMS aus, das Sie für die Verwendung des IAM-Dienstes installiert haben:
      - Wenn Sie MySQL oder MariaDB installiert haben, geben Sie "1" ein.
      - Wenn Sie PostgreSQL oder Postgres Pro installiert haben, geben Sie "2" ein.
   4. Geben Sie die Adresse des IAM-DBMS ein, die der IAM-Dienst verwenden soll.

5. Geben Sie die Portnummer des IAM-DBMS ein. Dieser Port wird für die Kommunikation mit dem IAM-Dienst verwendet. Standardmäßig werden die folgenden Ports verwendet:

   - Port 3306 für MySQL oder MariaDB
   - Port 5432 für PostgreSQL oder Postgres Pro

6. Geben Sie den Namen der IAM-Datenbank ein, den der IAM-Dienst verwenden soll. Der Name der vom IAM-Dienst verwendeten Datenbank muss sich von der Datenbank unterscheiden, die vom Administrationsserver verwendet wird.

3. **Aktualisieren Sie Kaspersky Security Center Web Console auf eine neue Version.**
4. **(Optional) Aktualisieren Sie die Administrationsagenten auf den Geräten auf eine neue Version.**
5. **Stellen Sie sicher, dass die Allow-Liste für die Zwei-Faktor-Authentifizierung nur die Benutzerkonten enthält, die Zugriff auf den Administrationsserver haben müssen.**

   Überprüfen Sie die Allow-Liste für Zwei-Faktor-Authentifizierung und entfernen Sie alle anderen Konten daraus.

Beachten Sie, dass Sie bei einer Aktualisierung des Administrationsservers auf Version 16.3 keine neuen Installationspakete des Administrationsagenten in Version 15 oder älter erstellen können. Bereits zuvor erstellte Installationspakete bleiben jedoch verfügbar.

Wenn Sie das Upgrade von Kaspersky Security Center Linux von einer älteren Version durchführen, werden alle installierten Plug-ins für unterstützte Kaspersky-Anwendungen beibehalten. Das Administrationsserver-Plug-in und Plug-in des Administrationsagenten werden automatisch aktualisiert.

Kaspersky Security Center Linux ab Version 16 aktualisieren

In diesem Abschnitt werden die folgenden Optionen für ein Upgrade von Kaspersky Security Center Linux ab Version 16 auf die aktuellste Version beschrieben:

- Upgrade mittels Installationsdatei
- Upgrade mittels Backup
- Upgrade auf den Knoten eines Kaspersky Security Center-Failover-Clusters

Kaspersky Security Center Linux ab Version 16 mittels Installationsdatei aktualisieren

Um den Administrationsserver ab Version 16 auf die aktuellste Version zu aktualisieren, können Sie mithilfe der Installationsdatei von Kaspersky Security Center Linux eine neue Version über die ältere installieren.

So aktualisieren Sie Kaspersky Security Center Linux ab Version 16 mithilfe der Installationsdatei auf die neueste Version:

1. Laden Sie die Installationsdatei für Kaspersky Security Center Linux mit einem vollständigen Paket für Version 16.3 von der Kaspersky-Website herunter:

   - Für Geräte mit einem RPM-basierten Betriebssystem – `ksc64-<Versionsnummer>.x86_64.rpm`
   - Für Geräte mit einem Debian-basierten Betriebssystem – `ksc64_<Versionsnummer>_amd64.deb`

2. Beginnen Sie mit dem Upgrade von Kaspersky Security Center Linux. Führen Sie in der Befehlszeile einen der folgenden Befehle aus:

   - Für Geräte mit einem RPM-basiertem Betriebssystem:

     ```
     sudo yum install ./ksc64-<Versionsnummer>.x86_64.rpm
     ```

   - Für Geräte mit einem Debian-basiertem Betriebssystem:

     ```
     sudo apt-get install ./ksc64_<Versionsnumemr>_amd64.deb
     ```

   Nachdem der Befehl erfolgreich ausgeführt wurde, wird das `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` erstellt. Eine entsprechende Meldung wird im Terminal angezeigt.

3. Führen Sie das Skript `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` aus, um den aktualisierten Administrationsserver zu konfigurieren.

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

4. Lesen Sie den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie, die im Befehlszeilenterminal angezeigt werden. Wenn Sie mit allen Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind:

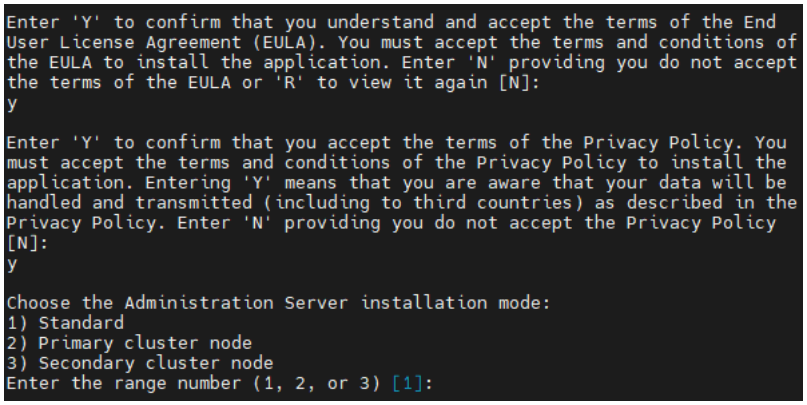
   a. Geben Sie `Y` ein, um zu bestätigen, dass Sie die Bedingungen der EULA vollständig gelesen und verstanden haben, und sie akzeptieren.

   b. Geben Sie erneut `Y` ein, um zu bestätigen, dass Sie die Datenschutzrichtlinie, die die Verarbeitung von Daten beschreibt, vollständig gelesen und verstanden haben, und sie akzeptieren.

   Nachdem Sie zwei Mal `Y` eingegeben haben, wird die Programminstallation auf Ihrem Gerät fortgesetzt.

5. Geben Sie `1` ein, um den Standard-Installationsmodus für den Administrationsserver auszuwählen.

Das folgende Bild zeigt die letzten beiden Schritte.



Akzeptieren der Bedingungen der EULA und der Datenschutzrichtlinie und Auswählen des Standard-Installationsmodus für den Administrationsserver im Befehlszeilenterminal

Anschließend wird das Administrationsserver-Upgrade vom Skript konfiguriert und abgeschlossen. Während des Upgrades können Sie die vor dem Upgrade geänderten Einstellungen des Administrationsservers nicht ändern.

6. Aktualisieren Sie Kaspersky Security Center Web Console auf eine neue Version.

7. Für die Geräte, auf denen bereits die frühere Version des Administrationsagenten installiert ist, erstellen und starten Sie die Aufgabe zur Remote-Installation der neuen Version des Administrationsagenten.

   Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center Linux.

   Nach Abschluss der Aufgabe zur Remote-Installation ist die Version des Administrationsagenten aktuell.

   Führen Sie die folgenden Befehle auf Linux-basierten Assets aus, um nicht mehr benötigte Abhängigkeiten zu entfernen:

   - Führen Sie für Debian-basierte Assets einen der folgenden Befehle aus:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Führen Sie für RPM-basierte Assets einen der folgenden Befehle aus:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

Kaspersky Security Center Linux ab Version 16 mittels Backup aktualisieren

Um den Administrationsserver ab Version 16 auf die aktuellste Version zu aktualisieren, können Sie ein Backup der Administrationsserver-Daten erstellen und diese Daten nach der Installation einer neuen Version von Kaspersky Security Center Linux wiederherstellen. Sollten bei der Installation Probleme auftreten, können Sie die vorherige Version des Administrationsservers wiederherstellen, indem Sie die vor dem Update erstellte Backup-Kopie der Administrationsserver-Daten heranziehen.

So aktualisieren Sie Kaspersky Security Center Linux ab Version 16 mithilfe eines Backups auf die neueste Version:

1. Erstellen Sie vor dem Upgrade ein Backup der Administrationsserver-Daten mit einer älteren Anwendungsversion.

2. Deinstallieren Sie die ältere Version von Kaspersky Security Center Linux.

3. Installieren Sie Kaspersky Security Center Linux Version 16.3 auf dem Gerät, auf dem der Administrationsserver vorher installiert war.

   Wenn sich das Datenbankschema in der Backup-Kopie von dem Schema unterscheidet, das derzeit vom Administrationsserver oder von IAM verwendet wird, werden die Daten nach dem aktuellen Schema wiederhergestellt.

   Wenn in der Backup-Kopie das Schema "public" verwendet wird, müssen folgende Bedingungen erfüllt sein:

   - Das Datenbankschema "public" ist in der Datenbank vorhanden.
   - Sie können das Datenbankschema "public" über das DBMS-Konto, das der Administrationsserver oder IAM für den Datenbankzugriff verwendet, ändern.

   Andernfalls wird die Datenwiederherstellung mit einem Fehler beendet.

4. Stellen Sie die Daten des Administrationsservers aus dem Backup, das vor dem Upgrade erstellt wurde, wieder her.

5. Installieren Sie die Kaspersky Security Center Web Console.

   Wenn die Kaspersky Security Center Web Console bereits installiert ist, installieren Sie die Web Console mit der gleichen Antwortdatei erneut.

   Melden Sie sich mit dem internen Benutzerkonto des Administrators an der Kaspersky Security Center Web Console an.

   Nach der Wiederherstellung der Daten des Administrationsservers dauert die Dateninitialisierung normalerweise bis zu 15 Minuten. Die genaue Zeit ist jedoch von der Hardwareleistung und vom Umfang der Daten des Administrationsservers abhängig. Während dieser Zeit kann die Kaspersky Security Center Web Console möglicherweise keine Verbindung herstellen und zeigt entsprechende Fehler an.

6. Für die Geräte, auf denen bereits die frühere Version des Administrationsagenten installiert ist, erstellen und starten Sie die Aufgabe zur Remote-Installation der neuen Version des Administrationsagenten.

   Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center Linux.

Nach Abschluss der Aufgabe zur Remote-Installation ist die Version des Administrationsagenten aktuell.

Führen Sie die folgenden Befehle auf Linux-basierten Assets aus, um nicht mehr benötigte Abhängigkeiten zu entfernen:

- Führen Sie für Debian-basierte Assets einen der folgenden Befehle aus:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- Führen Sie für RPM-basierte Assets einen der folgenden Befehle aus:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Kaspersky Security Center Linux ab Version 16 auf den Knoten des Kaspersky Security Center Linux Failover-Clusters aktualisieren

Sie können die aktuellste Version des Administrationsservers auf jedem Knoten eines Kaspersky Security Center Linux Failover-Clusters installieren, auf dem der Administrationsserver ab Version 16 installiert ist. Beim Aktualisieren auf die aktuellste Version bleiben alle Daten und Einstellungen der vorherigen Version des Administrationsservers erhalten.

Wenn Sie Kaspersky Security Center Linux zuvor lokal auf Geräten installiert haben, können Sie Kaspersky Security Center Linux auf diesen Geräten auch aktualisieren, indem Sie die Installationsdatei oder ein Backup verwenden.

So aktualisieren Sie Kaspersky Security Center Linux ab Version 16 auf den Knoten des Kaspersky Security Center Linux Failover-Clusters:

1. Laden Sie die Installationsdatei für Kaspersky Security Center Linux mit einem vollständigen Paket für Version 16.3 von der Kaspersky-Website herunter:
   - Für Geräte mit einem RPM-basierten Betriebssystem – `ksc64-<Versionsnummer>-<Build-Nummer>.x86_64.rpm`
   - Für Geräte mit einem Debian-basierten Betriebssystem – `ksc64_<Versionsnummer>-<Build-Nummer>_amd64.deb`
2. Halten Sie das Cluster an.

3. Um das Upgrade zu starten, führen Sie in der Befehlszeile des aktiven Cluster-Knotens den folgenden Befehl aus:

   - Für Geräte mit einem RPM-basiertem Betriebssystem:

     ```
     sudo yum install ./ksc64-<Versionsnummer>-<Build-Nummer>.x86_64.rpm
     ```

   - Für Geräte mit einem Debian-basiertem Betriebssystem:

     ```
     sudo apt-get install ./ksc64_<Versionsnummer>-<Build-Nummer>_amd64.deb
     ```

   Nachdem der Befehl erfolgreich ausgeführt wurde, wird das `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` erstellt. Eine entsprechende Meldung wird im Terminal angezeigt.

4. Führen Sie das Skript `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` aus, um den aktualisierten Administrationsserver zu konfigurieren.

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Lesen Sie den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie, die im Befehlszeilenterminal angezeigt werden. Wenn Sie mit allen Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind:

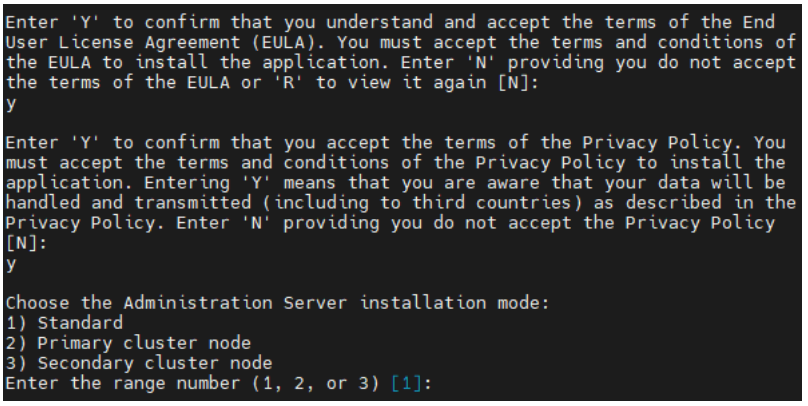
   a. Geben Sie `Y` ein, um zu bestätigen, dass Sie die Bedingungen der EULA vollständig gelesen und verstanden haben, und sie akzeptieren.

   b. Geben Sie erneut `Y` ein, um zu bestätigen, dass Sie die Datenschutzrichtlinie, die die Verarbeitung von Daten beschreibt, vollständig gelesen und verstanden haben, und sie akzeptieren.

   Nachdem Sie zwei Mal `Y` eingegeben haben, wird die Programminstallation auf Ihrem Gerät fortgesetzt.

6. Wählen Sie den Knoten aus, auf dem Sie das Upgrade durchführen, indem Sie `2` eingeben.

   Das folgende Bild zeigt die letzten beiden Schritte.



Akzeptieren der Bedingungen der EULA und der Datenschutzrichtlinie und Auswahl des Installationsmodus im Befehlszeilenterminal

Anschließend wird das Administrationsserver-Upgrade vom Skript konfiguriert und abgeschlossen. Während des Upgrades können Sie die vor dem Upgrade geänderten Einstellungen des Administrationsservers nicht ändern.

7. Führen Sie auf dem passiven Knoten den Schritt 5 aus.

   Geben Sie in Schritt 6 eine `3` ein, um den Knoten auszuwählen.

8. Starten Sie das Cluster.

   > Sie können den Cluster auf einem beliebigen Knoten starten. Wenn Sie den Cluster auf dem passiven Knoten starten, wird er zum aktiven Knoten.

9. Für die Geräte, auf denen die frühere Version des Administrationsagenten installiert ist, erstellen und starten Sie die Aufgabe zur Remote-Installation der neuen Version des Administrationsagenten.

   > Es wird empfohlen, den Administrationsagenten für Linux auf die Version von Kaspersky Security Center Linux zu aktualisieren.

   Nach Abschluss der Aufgabe zur Remote-Installation ist die Version des Administrationsagenten aktuell.

   Führen Sie die folgenden Befehle auf Linux-basierten Assets aus, um nicht mehr benötigte Abhängigkeiten zu entfernen:

   - Führen Sie für Debian-basierte Assets einen der folgenden Befehle aus:

     ```
     sudo apt-get -y autoremove
     ```

     ```
     sudo apt -y autoremove
     ```

   - Führen Sie für RPM-basierte Assets einen der folgenden Befehle aus:

     ```
     sudo dnf autoremove
     ```

     ```
     sudo yum autoremove
     ```

   Daraufhin haben Sie den Administrationsserver in der neusten Version auf den Knoten des Kaspersky Security Center Linux Failover-Clusters installiert.

Kaspersky Security Center Linux ab Version 15.4 oder früher aktualisieren

In diesem Abschnitt werden die folgenden Optionen für ein Upgrade von Kaspersky Security Center Linux Version 15.4 oder früher auf Version 16 oder höher beschrieben:

- Upgrade mittels Installationsdatei
- Upgrade mittels Backup
- Upgrade auf den Knoten eines Kaspersky Security Center-Failover-Clusters

Jede Upgrade-Option für Kaspersky Security Center Linux Version 15.4 oder niedriger auf Version 16 oder höher umfasst die folgenden Schritte: Erstellen und Konfigurieren einer IAM-Datenbank auf einem IAM-Server, Erstellen eines nicht privilegierten Kontos namens "ksciam" zur Ausführung des IAM-Dienstes, und das Hinzufügen dieses Kontos zur Sicherheitsgruppe "kladmins".

Kaspersky Security Center Linux Version 15.4 oder früher mittels Installationsdatei aktualisieren

Um den Administrationsserver der Version 14 – 15.4 auf die Version 16 oder höher zu aktualisieren, können Sie mithilfe der Installationsdatei von Kaspersky Security Center Linux eine neue Version über die ältere installieren.

Bevor Sie beginnen, **sehen Sie sich die Anforderungen an ein benutzerdefiniertes Zertifikat an**.

Wenn Sie anstelle des selbstsignierten Zertifikats ein benutzerdefiniertes Zertifikat verwenden, müssen Sie vor dem Upgrade von Kaspersky Security Center Linux auf die neuere Version sicherstellen, dass das Zertifikat den "Subject Alternative Name" (SAN) enthält. Wenn dies nicht der Fall ist, müssen Sie das Zertifikat unbedingt vor dem Upgrade von Kaspersky Security Center Linux ersetzen. Andernfalls können Sie sich nach dem Upgrade nicht mehr in der Webkonsole anmelden.

Um sicherzustellen, dass das Zertifikat den SAN enthält:

1. Führen Sie auf dem Gerät mit dem installierten Administrationsserver folgenden Befehl aus:

   - Für ein Linux-Gerät:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Für ein Windows-Gerät:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Stellen Sie sicher, dass der "Subject Alternative Name" in der Befehlsausgabe angezeigt wird und die Adresse des Administrationsservergeräts enthält.

3. Falls der "Subject Alternative Name" nicht angezeigt wird, verwenden Sie das Tool klsetsrvcert, um Ihr benutzerdefiniertes Zertifikat durch ein Zertifikat zu ersetzen, dass die Anforderungen erfüllt.

So aktualisieren Sie Kaspersky Security Center Linux Version 15.4 oder früher mithilfe der Installationsdatei auf die neueste Version:

1. Laden Sie die Installationsdatei für Kaspersky Security Center Linux mit einem vollständigen Paket für Version 16.3 von der Kaspersky-Website herunter:

   - Für Geräte mit einem RPM-basierten Betriebssystem – `ksc64-<Versionsnummer>.x86_64.rpm`
   - Für Geräte mit einem Debian-basierten Betriebssystem – `ksc64_<Versionsnummer>_amd64.deb`

2. Erstellen Sie auf DBMS-Server eine Datenbank für IAM. Der Name der IAM-Datenbank muss sich von der Datenbank unterscheiden, die vom Administrationsserver verwendet wird.

   - Für PostgreSQL führen Sie den folgenden Befehl aus:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <Name_der_IAM_DB>;"
     ```

- Für MariaDB führen Sie den folgenden Befehl aus:

```
sudo mysql -u root -p -e "CREATE DATABASE <Name_der_IAM_DB>;"
```

3. Erstellen Sie ein nicht privilegiertes Konto namens "ksciam", fügen Sie es der Sicherheitsgruppe "kladmins" hinzu und legen Sie anschließend die Gruppe "kladmins" als primäre Gruppe für das Konto "ksciam" fest. Führen Sie dazu nacheinander die folgenden Befehle aus:

```
sudo adduser ksciam
sudo gpasswd -a ksciam kladmins
sudo usermod -g kladmins ksciam
```

4. Beginnen Sie mit dem Upgrade von Kaspersky Security Center Linux. Führen Sie in der Befehlszeile einen der folgenden Befehle aus:

   - Für Geräte mit einem RPM-basiertem Betriebssystem:

   ```
   sudo yum install ./ksc64-<Versionsnummer>.x86_64.rpm
   ```

   - Für Geräte mit einem Debian-basiertem Betriebssystem:

   ```
   sudo apt-get install ./ksc64_<Versionsnummer>_amd64.deb
   ```

   Nachdem der Befehl erfolgreich ausgeführt wurde, wird das `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` erstellt. Eine entsprechende Meldung wird im Terminal angezeigt.

5. Führen Sie das Skript `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` aus, um den aktualisierten Administrationsserver zu konfigurieren.

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

6. Lesen Sie den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie, die im Befehlszeilenterminal angezeigt werden. Wenn Sie mit allen Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind:

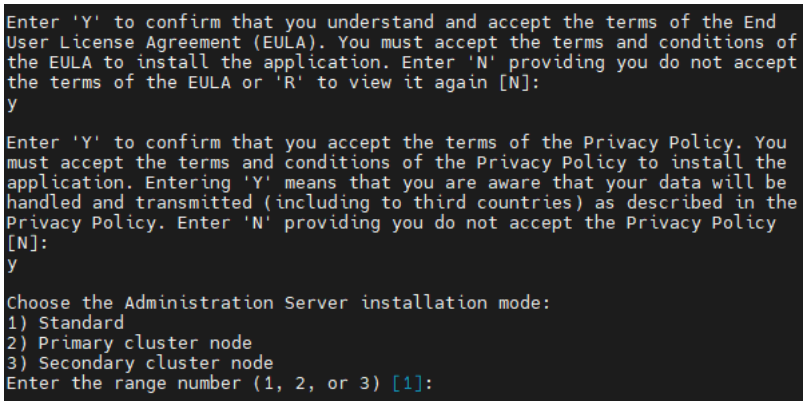
   a. Geben Sie `Y` ein, um zu bestätigen, dass Sie die Bedingungen der EULA vollständig gelesen und verstanden haben, und sie akzeptieren.

   b. Geben Sie erneut `Y` ein, um zu bestätigen, dass Sie die Datenschutzrichtlinie, die die Verarbeitung von Daten beschreibt, vollständig gelesen und verstanden haben, und sie akzeptieren.

   Nachdem Sie zwei Mal `Y` eingegeben haben, wird die Programminstallation auf Ihrem Gerät fortgesetzt.

7. Geben Sie `1` ein, um den Standard-Installationsmodus für den Administrationsserver auszuwählen.

Das folgende Bild zeigt die letzten beiden Schritte.



Akzeptieren der Bedingungen der EULA und der Datenschutzrichtlinie und Auswählen des Standard-Installationsmodus für den Administrationsserver im Befehlszeilenterminal

8. Anschließend wird das Administrationsserver-Upgrade vom Skript konfiguriert und abgeschlossen. Während des Upgrades können Sie die vor dem Upgrade geänderten Einstellungen des Administrationsservers nicht ändern. Geben Sie nach der entsprechenden Aufforderung die folgenden Einstellungen ein:

   a. Geben Sie den FQDN des IAM-Servers ein.

      Sie müssen den DNS-Namen des Administrationsservers verwenden, der bei der Installation von Kaspersky Security Center Linux angegeben wurde.

   b. Geben Sie den Namen des Kontos ein, um den IAM-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto "ksciam" verwendet.

   c. Wählen Sie das DBMS aus, das Sie für die Verwendung des IAM-Dienstes installiert haben:

      - Wenn Sie MySQL oder MariaDB installiert haben, geben Sie `1` ein.
      - Wenn Sie PostgreSQL oder Postgres Pro installiert haben, geben Sie `2` ein.

   d. Geben Sie die Adresse des IAM-DBMS ein, die der IAM-Dienst verwenden soll.

   e. Geben Sie die Portnummer des IAM-DBMS ein. Dieser Port wird für die Kommunikation mit dem IAM-Dienst verwendet. Standardmäßig werden die folgenden Ports verwendet:

      - Port 3306 für MySQL oder MariaDB
      - Port 5432 für PostgreSQL oder Postgres Pro

   f. Geben Sie den Namen der IAM-Datenbank ein, den der IAM-Dienst verwenden soll. Der Name der vom IAM-Dienst verwendeten Datenbank muss sich von der Datenbank unterscheiden, die vom Administrationsserver verwendet wird.

   g. Geben Sie den DBMS-Login und das Kennwort ein, die vom IAM-Dienst verwendet werden.

   h. Wenn Sie PostgreSQL oder Postgres Pro installiert haben, können Sie das Datenbankschema, das von IAM verwendet werden soll, festlegen. Geben Sie dazu den Namen des Schemas an.

      Wenn Sie kein benutzerdefiniertes Schema verwenden möchten, drücken Sie `ENTER`. Dadurch wird ein Schema "public" verwendet.

Beim Namen des Schemas wird die Groß- und Kleinschreibung berücksichtigt: Sie dürfen nur Kleinbuchstaben verwenden.
Die folgenden Namen sind bereits von IAM reserviert und dürfen ebenfalls nicht angegeben werden: `client, iam, ksc, locker, pat, scope, voltron`.

9. Aktualisieren Sie Kaspersky Security Center Web Console auf eine neue Version.
10. Für die Geräte, auf denen bereits die frühere Version des Administrationsagenten installiert ist, erstellen und starten Sie die Aufgabe zur Remote-Installation der neuen Version des Administrationsagenten.

    Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center Linux.

    Nach Abschluss der Aufgabe zur Remote-Installation ist die Version des Administrationsagenten aktuell.

    Führen Sie die folgenden Befehle auf Linux-basierten Assets aus, um nicht mehr benötigte Abhängigkeiten zu entfernen:

    - Führen Sie für Debian-basierte Assets einen der folgenden Befehle aus:

      ```
      sudo apt-get -y autoremove
      ```

      ```
      sudo apt -y autoremove
      ```

    - Führen Sie für RPM-basierte Assets einen der folgenden Befehle aus:

      ```
      sudo dnf autoremove
      ```

      ```
      sudo yum autoremove
      ```

Kaspersky Security Center Linux Version 15.4 oder früher mittels Backup aktualisieren

Um den Administrationsserver Version 14.2 – 15.4 auf Version 16 oder höher zu aktualisieren, können Sie ein Backup der Daten des Administrationsservers erstellen und diese Daten nach der Installation einer neuen Version von Kaspersky Security Center Linux wiederherstellen. Sollten bei der Installation Probleme auftreten, können Sie die vorherige Version des Administrationsservers wiederherstellen, indem Sie die vor dem Update erstellte Backup-Kopie der Administrationsserver-Daten heranziehen.

Erforderliche Vorrausetzungen

1. **Prüfen Sie die Anforderungen an ein benutzerdefiniertes Zertifikat**.

   Wenn Sie anstelle des selbstsignierten Zertifikats ein benutzerdefiniertes Zertifikat verwenden, müssen Sie vor dem Upgrade von Kaspersky Security Center Linux auf die neuere Version sicherstellen, dass das Zertifikat den "Subject Alternative Name" (SAN) enthält. Wenn dies nicht der Fall ist, müssen Sie das Zertifikat unbedingt vor dem Upgrade von Kaspersky Security Center Linux ersetzen. Andernfalls können Sie sich nach dem Upgrade nicht mehr in der Webkonsole anmelden.

   Um sicherzustellen, dass das Zertifikat den SAN enthält:

   1. Führen Sie auf dem Gerät mit dem installierten Administrationsserver folgenden Befehl aus:

      - Für ein Linux-Gerät:

        ```
        sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
        ```

      - Für ein Windows-Gerät:

        ```
        certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
        ```

   2. Stellen Sie sicher, dass der "Subject Alternative Name" in der Befehlsausgabe angezeigt wird und die Adresse des Administrationsservergeräts enthält.

   3. Falls der "Subject Alternative Name" nicht angezeigt wird, verwenden Sie das Tool klsetsrvcert, um Ihr benutzerdefiniertes Zertifikat durch ein Zertifikat zu ersetzen, dass die Anforderungen erfüllt.

2. Erstellen Sie ein Backup der Administrationsserver-Daten mit einer älteren Version der Anwendung.

Der Upgrade-Prozess

So aktualisieren Sie Kaspersky Security Center Linux Version 15.4 oder früher mithilfe eines Backups auf die neueste Version:

1. Deinstallieren Sie die ältere Version von Kaspersky Security Center Linux.

2. Erstellen Sie auf DBMS-Server eine Datenbank für IAM. Der Name der IAM-Datenbank muss sich von der Datenbank unterscheiden, die vom Administrationsserver verwendet wird.

   - Für PostgreSQL führen Sie den folgenden Befehl aus:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <Name_der_IAM_DB>;"
     ```

   - Für MariaDB führen Sie den folgenden Befehl aus:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <Name_der_IAM_DB>;"
     ```

3. Erstellen Sie ein nicht privilegiertes Konto namens "ksciam", fügen Sie es der Sicherheitsgruppe "kladmins" hinzu und legen Sie anschließend die Gruppe "kladmins" als primäre Gruppe für das Konto "ksciam" fest. Führen Sie dazu nacheinander die folgenden Befehle aus:

```
sudo adduser ksciam
sudo gpasswd -a ksciam kladmins
sudo usermod -g kladmins ksciam
```

4. Installieren Sie Kaspersky Security Center Linux Version 16.3 auf dem Gerät, auf dem der Administrationsserver vorher installiert war.

   Wenn sich das Datenbankschema in der Backup-Kopie von dem Schema unterscheidet, das derzeit vom Administrationsserver oder von IAM verwendet wird, werden die Daten nach dem aktuellen Schema wiederhergestellt.

   Wenn in der Backup-Kopie das Schema "public" verwendet wird, müssen folgende Bedingungen erfüllt sein:

   - Das Datenbankschema "public" ist in der Datenbank vorhanden.
   - Sie können das Datenbankschema "public" über das DBMS-Konto, das der Administrationsserver oder IAM für den Datenbankzugriff verwendet, ändern.

   Andernfalls wird die Datenwiederherstellung mit einem Fehler beendet.

5. Stellen Sie die Daten des Administrationsservers aus dem Backup, das vor dem Upgrade erstellt wurde, wieder her.

6. Konfigurieren Sie die Überprüfung des Zertifikats durch Administrationsserver und IAM-Server.

7. Installieren Sie die Kaspersky Security Center Web Console.

   Wenn die Kaspersky Security Center Web Console bereits installiert ist, installieren Sie die Web Console mit der gleichen Antwortdatei erneut.

   Melden Sie sich mit dem internen Benutzerkonto des Administrators an der Kaspersky Security Center Web Console an.

   Nach der Wiederherstellung der Daten des Administrationsservers dauert die Dateninitialisierung normalerweise bis zu 15 Minuten. Die genaue Zeit ist jedoch von der Hardwareleistung und vom Umfang der Daten des Administrationsservers abhängig. Während dieser Zeit kann die Kaspersky Security Center Web Console möglicherweise keine Verbindung herstellen und zeigt entsprechende Fehler an.

8. Für die Geräte, auf denen bereits die frühere Version des Administrationsagenten installiert ist, erstellen und starten Sie die Aufgabe zur Remote-Installation der neuen Version des Administrationsagenten.

   > Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center Linux.

   Nach Abschluss der Aufgabe zur Remote-Installation ist die Version des Administrationsagenten aktuell.

Führen Sie die folgenden Befehle auf Linux-basierten Assets aus, um nicht mehr benötigte Abhängigkeiten zu entfernen:

- Führen Sie für Debian-basierte Assets einen der folgenden Befehle aus:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- Führen Sie für RPM-basierte Assets einen der folgenden Befehle aus:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Kaspersky Security Center Linux Version 15.4 oder früher auf den Knoten des Kaspersky Security Center Linux Failover-Clusters aktualisieren

Sie können den Administrationsserver ab Version 16 auf jeden Knoten des Kaspersky Security Center-Failover-Clusters installieren, auf dem der Administrationsserver der Version 14 – 15.4 installiert ist. Beim Aktualisieren bleiben alle Daten und Einstellungen der vorherigen Version des Administrationsservers erhalten.

Bevor Sie beginnen, **sehen Sie sich die Anforderungen an ein benutzerdefiniertes Zertifikat an**.

Wenn Sie anstelle des selbstsignierten Zertifikats ein benutzerdefiniertes Zertifikat verwenden, müssen Sie vor dem Upgrade von Kaspersky Security Center Linux auf die neuere Version sicherstellen, dass das Zertifikat den "Subject Alternative Name" (SAN) enthält. Wenn dies nicht der Fall ist, müssen Sie das Zertifikat unbedingt vor dem Upgrade von Kaspersky Security Center Linux ersetzen. Andernfalls können Sie sich nach dem Upgrade nicht mehr in der Webkonsole anmelden.

Um sicherzustellen, dass das Zertifikat den SAN enthält:

1. Führen Sie auf dem Gerät mit dem installierten Administrationsserver folgenden Befehl aus:

   - Für ein Linux-Gerät:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Für ein Windows-Gerät:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Stellen Sie sicher, dass der "Subject Alternative Name" in der Befehlsausgabe angezeigt wird und die Adresse des Administrationsservergeräts enthält.

3. Falls der "Subject Alternative Name" nicht angezeigt wird, verwenden Sie das Tool klsetsrvcert, um Ihr benutzerdefiniertes Zertifikat durch ein Zertifikat zu ersetzen, dass die Anforderungen erfüllt.

Wenn Sie Kaspersky Security Center Linux zuvor lokal auf Geräten installiert haben, können Sie Kaspersky Security Center Linux auf diesen Geräten auch aktualisieren, indem Sie die Installationsdatei oder ein Backup verwenden.

So aktualisieren Sie Kaspersky Security Center Linux Version 15.4 oder früher auf den Knoten des Kaspersky Security Center Linux Failover-Clusters:

1. Laden Sie die Installationsdatei für Kaspersky Security Center Linux mit einem vollständigen Paket für Version 16.3 von der Kaspersky-Website herunter:

   - Für Geräte mit einem RPM-basierten Betriebssystem – `ksc64-<Versionsnummer>-<Build-Nummer>.x86_64.rpm`
   - Für Geräte mit einem Debian-basierten Betriebssystem – `ksc64_<Versionsnummer>-<Build-Nummer>_amd64.deb`

2. Halten Sie das Cluster an.

3. Erstellen Sie auf DBMS-Server eine Datenbank für IAM. Der Name der IAM-Datenbank muss sich von der Datenbank unterscheiden, die vom Administrationsserver verwendet wird.

   - Für PostgreSQL führen Sie den folgenden Befehl aus:

     ```
     sudo -i -u postgres psql -U postgres -c "CREATE DATABASE <Name_der_IAM_DB>;"
     ```

   - Für MariaDB führen Sie den folgenden Befehl aus:

     ```
     sudo mysql -u root -p -e "CREATE DATABASE <Name_der_IAM_DB>;"
     ```

4. Erstellen Sie ein nicht privilegiertes Konto namens "ksciam", fügen Sie es der Sicherheitsgruppe "kladmins" hinzu und legen Sie anschließend die Gruppe "kladmins" als primäre Gruppe für das Konto "ksciam" fest. Führen Sie dazu nacheinander die folgenden Befehle aus:

   ```
   sudo adduser ksciam
   sudo gpasswd -a ksciam kladmins
   sudo usermod -g kladmins ksciam
   ```

5. Um das Upgrade zu starten, führen Sie in der Befehlszeile des aktiven Cluster-Knotens einen der folgenden Befehle aus:

   - Für Geräte mit einem RPM-basiertem Betriebssystem:

     ```
     sudo yum install ./ksc64-<Versionsnummer>-<Build-Nummer>.x86_64.rpm
     ```

- Für Geräte mit einem Debian-basiertem Betriebssystem:

```
sudo apt-get install ./ksc64_<Versionsnummer>-<Build-Nummer>_amd64.deb
```

Nachdem der Befehl erfolgreich ausgeführt wurde, wird das `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` erstellt. Eine entsprechende Meldung wird im Terminal angezeigt.

6. Führen Sie das Skript `/opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl` aus, um den aktualisierten Administrationsserver zu konfigurieren.

```
sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
```

7. Lesen Sie den Endbenutzer-Lizenzvertrag und die Datenschutzrichtlinie, die im Befehlszeilenterminal angezeigt werden. Wenn Sie mit allen Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie einverstanden sind:

   a. Geben Sie `Y` ein, um zu bestätigen, dass Sie die Bedingungen der EULA vollständig gelesen und verstanden haben, und sie akzeptieren.

   b. Geben Sie erneut `Y` ein, um zu bestätigen, dass Sie die Datenschutzrichtlinie, die die Verarbeitung von Daten beschreibt, vollständig gelesen und verstanden haben, und sie akzeptieren.

   Nachdem Sie zwei Mal `Y` eingegeben haben, wird die Programminstallation auf Ihrem Gerät fortgesetzt.

8. Wählen Sie den Knoten aus, auf dem Sie das Upgrade durchführen, indem Sie `2` eingeben.

   Das folgende Bild zeigt die letzten beiden Schritte.

```
Enter 'Y' to confirm that you understand and accept the terms of the End
User License Agreement (EULA). You must accept the terms and conditions of
the EULA to install the application. Enter 'N' providing you do not accept
the terms of the EULA or 'R' to view it again [N]:
y

Enter 'Y' to confirm that you accept the terms of the Privacy Policy. You
must accept the terms and conditions of the Privacy Policy to install the
application. Entering 'Y' means that you are aware that your data will be
handled and transmitted (including to third countries) as described in the
Privacy Policy. Enter 'N' providing you do not accept the Privacy Policy
[N]:
y

Choose the Administration Server installation mode:
1) Standard
2) Primary cluster node
3) Secondary cluster node
Enter the range number (1, 2, or 3) [1]:
```

Akzeptieren der Bedingungen der EULA und der Datenschutzrichtlinie und Auswahl des Installationsmodus im Befehlszeilenterminal

9. Anschließend wird das Administrationsserver-Upgrade vom Skript konfiguriert und abgeschlossen. Während des Upgrades können Sie die vor dem Upgrade geänderten Einstellungen des Administrationsservers nicht ändern. Geben Sie nach der entsprechenden Aufforderung die folgenden Einstellungen ein:

   a. Geben Sie den FQDN des IAM-Servers ein.

   Sie müssen den DNS-Namen des Administrationsservers verwenden, der bei der Installation von Kaspersky Security Center Linux angegeben wurde.

   b. Geben Sie den Namen des Kontos ein, um den IAM-Dienst zu starten. Das Konto muss Mitglied der eingegebenen Sicherheitsgruppe sein. Standardmäßig wird das Konto "ksciam" verwendet.

c. Wählen Sie das DBMS aus, das Sie für die Verwendung des IAM-Dienstes installiert haben:

- Wenn Sie MySQL oder MariaDB installiert haben, geben Sie `1` ein.
- Wenn Sie PostgreSQL oder Postgres Pro installiert haben, geben Sie `2` ein.

d. Geben Sie die Adresse des IAM-DBMS ein, die der IAM-Dienst verwenden soll.

e. Geben Sie die Portnummer des IAM-DBMS ein. Dieser Port wird für die Kommunikation mit dem IAM-Dienst verwendet. Standardmäßig werden die folgenden Ports verwendet:

- Port 3306 für MySQL oder MariaDB
- Port 5432 für PostgreSQL oder Postgres Pro

f. Geben Sie den Namen der IAM-Datenbank ein, den der IAM-Dienst verwenden soll. Der Name der vom IAM-Dienst verwendeten Datenbank muss sich von der Datenbank unterscheiden, die vom Administrationsserver verwendet wird.

g. Geben Sie den DBMS-Login und das Kennwort ein, die vom IAM-Dienst verwendet werden.

10. Führen Sie auf dem passiven Knoten den Schritt 5 aus.

    Geben Sie in Schritt 6 eine `3` ein, um den Knoten auszuwählen.

11. Starten Sie das Cluster.

    > Sie können den Cluster auf einem beliebigen Knoten starten. Wenn Sie den Cluster auf dem passiven Knoten starten, wird er zum aktiven Knoten.

12. Für die Geräte, auf denen die frühere Version des Administrationsagenten installiert ist, erstellen und starten Sie die Aufgabe zur Remote-Installation der neuen Version des Administrationsagenten.

    > Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center Linux.

    Nach Abschluss der Aufgabe zur Remote-Installation ist die Version des Administrationsagenten aktuell.

    Führen Sie die folgenden Befehle auf Linux-basierten Assets aus, um nicht mehr benötigte Abhängigkeiten zu entfernen:

- Führen Sie für Debian-basierte Assets einen der folgenden Befehle aus:

```
sudo apt-get -y autoremove
```

```
sudo apt -y autoremove
```

- Führen Sie für RPM-basierte Assets einen der folgenden Befehle aus:

```
sudo dnf autoremove
```

```
sudo yum autoremove
```

Daraufhin haben Sie den Administrationsserver in der neusten Version auf den Knoten des Kaspersky Security Center Linux Failover-Clusters installiert.

Aktualisieren von Kaspersky Security Center Web Console

In diesem Artikel wird beschrieben, wie Sie den Server der Web Console von Kaspersky Security Center (auch "Kaspersky Security Center Web Console" genannt) auf Geräten mit Linux-Betriebssystemen aktualisieren.

Wenn Sie Kaspersky Security Center Web Console unter Astra Linux in der abgeschlossenen Softwareumgebung aktualisieren, befolgen Sie die spezifischen Anweisungen für Astra Linux.

Verwenden Sie eine der folgenden Installationsdateien, je nach der Linux-Distribution, die auf Ihrem Gerät installiert ist:

- Für Debian: ksc-web-console-<Build-Nummer>.x86_64.deb
- Für RPM-basierte Betriebssysteme: ksc-web-console-<Build-Nummer>.x86_64.rpm

Die Installationsdatei können Sie diese von der Kaspersky-Website herunterladen.

So aktualisieren Sie Kaspersky Security Center Web Console:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center Web Console aktualisieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.
2. Lesen und akzeptieren Sie den Endbenutzer-Lizenzvertrag (EULA). Wenn das Programmpaket von Kaspersky Security Center Linux keine txt-Datei mit dem Text der EULA enthält, können Sie die Datei von der Kaspersky-Website herunterladen. Wenn Sie die Bedingungen des Lizenzvertrags nicht akzeptieren, können Sie Kaspersky Security Center Web Console nicht mithilfe der Installationsdatei aktualisieren.
3. Verwenden Sie die Antwortdatei, die Sie vor der Installation von Kaspersky Security Center Web Console vorbereitet haben. Die Datei heißt "ksc-web-console-setup.json" und befindet sich unter "/etc/ksc-web-console-setup.json".

   Wenn Sie bei der Installation von Kaspersky Security Center Web Console Werte für die Parameter `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, `messageQueueAccount` und `natsMessageQueueAccount` angegeben haben, stellen Sie sicher, dass alle diese Parameter in der Antwortdatei angegeben sind.

Wenn die Antwortdatei nicht vorhanden ist, erstellen Sie eine neue Antwortdatei, in der die Parameter für die Verbindung von Kaspersky Security Center Web Console mit dem Administrationsserver enthalten sind. Geben Sie der Datei den Namen "ksc-web-console-setup.json" und speichern Sie diese anschließend im Verzeichnis "/etc".

Beispiel für eine Antwortdatei mit den minimal notwendigen Parametern

Die Gruppe an Parametern in der Antwortdatei hängt von der Version des Administrationsservers ab, mit welcher die Kaspersky Security Center Web Console verbunden ist:

- Administrationsserver ab Version 16

  Beispiel für eine Antwortdatei mit minimalen Parametern für die Anmeldung am Administrationsserver Version 16 oder höher:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Administrationsserver Version 15.4 oder niedriger

  Beispiel für eine Antwortdatei mit minimalen Parametern für die Anmeldung am Administrationsserver Version 15.4 oder niedriger:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Sie können die Kaspersky Security Center Web Console entweder auf demselben Gerät, auf dem der Administrationsserver installiert ist, oder auf einem anderen Gerät installieren. Wenn die Kaspersky Security Center Web Console auf einem anderen Gerät installiert ist, unterscheidet sich die Adresse der Kaspersky Security Center Web Console (durch `address` angegeben) von der Adresse des Administrationsservers (durch `iamHost` oder `kscHost` angegeben). Wenn die Kaspersky Security Center Web Console und der Administrationsserver auf demselben Gerät installiert sind, besitzen diese Parameter die gleichen Werte.

Der Wert `iamHost` muss mit der IAM-Adresse übereinstimmen, die Sie bei der Installation des Administrationsservers angegeben haben. Um die angegebene IAM-Adresse zu erhalten, führen Sie folgenden Befehl auf dem Gerät mit dem installierten Administrationsserver aus:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Weiter Informationen dazu finden Sie in folgendem Artikel: Installationsparameter für Kaspersky Security Center Web Console.

Sie können der Liste der vertrauenswürdigen Server mehrere Administrationsserver unterschiedlicher Versionen hinzufügen. In diesem Fall können die Server unterschiedliche Authentifizierungsmethoden verwenden.

Wenn Sie eine Kaspersky Security Center Web Console aktualisieren möchten, die mit einem auf den Knoten des Kaspersky Security Center Linux Failover-Clusters installierten Administrationsserver verbunden ist, geben Sie in der Antwortdatei den Installationsparameter "trusted" an. Dies ist notwendig, damit der Kaspersky Security Center Linux-Failover-Cluster eine Verbindung mit der Kaspersky Security Center Web Console herstellen kann.

Komponenten des **Installationsparameters** `trusted`

Wenn Sie für die Verbindung mit einem Kaspersky Security Center Linux Failover-Cluster die Domänenauthentifizierung mit SSO verwenden, geben Sie die vertrauenswürdigen Installationsparameter wie folgt an: Wenn Sie die Kaspersky Security Center Web Console mit einem Administrationsserver der Version 16 oder höher verbinden, wird die durch die Identitäts- und Zugriffsverwaltung (IAM) bereitgestellte Domänenauthentifizierung mit einmaliger Anmeldung (SSO) verwendet. Geben Sie in diesem Fall die Installationsparameter für `trusted` wie folgt an:

```
"trusted":  {
  "<Name des Administrationsservers>": {
    "iamHost": "ksc-iam.example.com",
    "iamOAuthPort": 4444,
    "iamProxyPort": 9050,
    "iamCertPath": "<gemeinsamer Ordner für Daten>/iam/main_certificate.pem",
    "iamPATPath": "<gemeinsamer Ordner für Daten>/iam/initial_token.txt",
    "kscPort": 13299,
    "kscCertPath": "<gemeinsamer Ordner für Daten>/1093/cert/klserver.cer"
  }
}
```

wobei:

- `<Name des Administrationsservers>` dem Namen des Kaspersky Security Center Linux Failover-Clusters entspricht, der im Anmeldefenster der Kaspersky Security Center Web Console angezeigt wird.

- `iamHost` der Adresse des Geräts mit installiertem Administrationsserver und IAM entspricht. Wenn Sie im Rahmen der Vorbereitung der Cluster-Knoten einen sekundären Netzwerkadapter erstellt haben, verwenden Sie die FQDN oder den Hostnamen des Adapters als Adresse für das Kaspersky Security Center Linux Failover-Cluster. Geben Sie andernfalls die FQDN oder den Hostnamen des von Ihnen verwendeten Load Balancers eines Drittanbieters an.

  Der Wert `iamHost` muss mit der IAM-Adresse übereinstimmen, die bei der Installation des Administrationsservers angegeben wurde. Um die angegebene IAM-Adresse zu erhalten, führen Sie folgenden Befehl auf dem Host des Administrationsservers aus:

  ```
  grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
  ```

- `iamOAuthPort` dem Port entspricht, der für den Austausch der Authentifizierungstoken über das OpenID Connect-Authentifizierungsprotokoll verwendet wird (der Standardwert beträgt 4444). Dieser Port wird sowohl für die Kommunikation zwischen dem Server der Kaspersky Security Center Web Console und dem Administrationsserver als auch zwischen dem Browser (in dem Kaspersky Security Center Web Console verwendet wird) und dem Administrationsserver verwendet.

- `iamProxyPort` dem Port entspricht, der zur Verbindung des Servers der Kaspersky Security Center Web Console mit dem Administrationsserver verwendet wird (der Standardwert beträgt 9050).

- `iamCertPath` dem Pfad zum IAM-Zertifikat entspricht. Das IAM-Zertifikat wird beim ersten Start des Administrationsservers automatisch erstellt. Die Zertifikatsdatei befindet sich auf dem Gerät, auf dem der Administrationsserver installiert ist. Der Standardpfad des Zertifikats lautet: `< gemeinsamer Ordner für Daten >/iam/main_certificate.pem`. Das Zertifikat befindet sich im freigegebenen Datenspeicher des Kaspersky Security Center Linux Failover-Clusters. Das selbstsignierte IAM-Zertifikat wird automatisch rotiert.

- `iamPATPath` dem Pfad des Tokens entspricht, der für die Registrierung der Kaspersky Security Center Web Console als OAuth-Client in der IAM verwendet wird. Die Datei wird beim ersten Start des Administrationsservers erstellt. Das Token befindet sich auf dem Gerät mit dem installierten Administrationsserver. Der Standardpfad des Tokens lautet: <gemeinsamer Ordner für Daten>/iam/initial_token.txt. Das Token befindet sich im freigegebenen Datenspeicher des Kaspersky Security Center Linux Failover-Clusters. Das Token ist unbegrenzt gültig und erfordert keine Rotation.

- `kscPort` dem OpenAPI-Port entspricht, den Kaspersky Security Center Web Console für die Verbindung mit dem Administrationsserver verwendet (Standardwert ist 13299).

- `kscCertPath` dem Zertifikat des Administrationsservers entspricht, das sich im freigegebenen Datenspeicher des Kaspersky Security Center Linux Failover-Clusters befindet. Der Standardpfad zur Zertifikatsdatei lautet: `< gemeinsamer Ordner für Daten >\1093\cert\klserver.cer`.

  > Kopieren Sie Dateien des Zertifikats des Administrationsservers (angegeben durch `kscCertPath`), des IAM-Zertifikats (angegeben durch `iamCertPath`) und des Tokens (angegeben durch `iamPATPath`) vom gemeinsamen Datenspeicher auf das Gerät, auf dem Sie die Kaspersky Security Center Web Console installieren. Geben Sie den lokalen Pfad zum Zertifikat des Administrationsservers an.

Wenn Sie die Kaspersky Security Center Web Console mit einem Administrationsserver der Version 15.4 oder niedriger verbinden, wird die Authentifizierung unter Angabe von Name und Kennwort des Domänenbenutzers oder des internen Benutzers verwendet. Geben Sie in diesem Fall die vertrauenswürdigen Installationsparameter wie folgt an:

```
"trusted":  {
  "<Name des Administrationsservers>": {
    "kscHost": "ksc.example.com",
    "kscPort": 13299,
    "kscCertPath": "<gemeinsamer Ordner für Daten>/1093/cert/klserver.cer"
  }
}
```

wobei:

- `< Name des Administrationsservers >` dem Namen des Kaspersky Security Center Linux Failover-Clusters entspricht, der im Anmeldefenster der Kaspersky Security Center Web Console angezeigt wird.

- `kscHost` der Adresse (FQDN oder Hostname) des Administrationsservers entspricht. Wenn Sie im Rahmen der Vorbereitung der Cluster-Knoten einen sekundären Netzwerkadapter erstellt haben, verwenden Sie die Adresse des Adapters als Adresse für das Kaspersky Security Center Linux Failover-Cluster. Geben Sie andernfalls die Adresse eines von Ihnen verwendeten Load Balancers eines Drittanbieters an.

- `kscPort` dem OpenAPI-Port entspricht, den Kaspersky Security Center Web Console für die Verbindung mit dem Administrationsserver verwendet (Standardwert ist 13299).

- `kscCertPath` dem Zertifikat des Administrationsservers entspricht, das sich im freigegebenen Datenspeicher des Kaspersky Security Center Linux Failover-Clusters befindet. Der Standardpfad zur Zertifikatsdatei lautet: `< gemeinsamer Ordner für Daten >\1093\cert\klserver.cer`. Kopieren Sie die Zertifikatsdatei aus dem freigegebenen Datenspeicher auf das Gerät, auf dem Sie Kaspersky Security Center Web Console installieren. Geben Sie den lokalen Pfad zum Zertifikat des Administrationsservers an.

Kaspersky Security Center Web Console kann nicht aktualisiert werden, wenn dafür dieselbe Installationsdatei verwendet wird. Wenn Sie die Einstellungen in einer Antwortdatei ändern und diese Datei zur Neuinstallation der Anwendung verwenden möchten, müssen Sie die Anwendung zunächst entfernen und sie anschließend mit der neuen Antwortdatei erneut installieren.

4. Führen Sie unter einem Benutzerkonto mit Root-Berechtigungen mithilfe der Befehlszeile und abhängig von Ihrer Linux-Distribution die Setup-Datei mit der Erweiterung .deb oder .rpm aus.

   Um eine ältere Version von Kaspersky Security Center Web Console zu aktualisieren, führen Sie einen der folgenden Befehle aus:

   - Für Geräte mit einem RPM-basiertem Betriebssystem:
     ```
     sudo yum install ksc-web-console-<Build-Nummer>.x86_64.rpm
     ```
   - Für Geräte mit einem Debian-basiertem Betriebssystem:
     ```
     sudo apt-get install ksc-web-console-<Build-Nummer>.x86_64.deb
     ```

   Dadurch wird die Setup-Datei entpackt. Bitte warten Sie, bis die Installation abgeschlossen ist.

5. Starten Sie alle Dienste von Kaspersky Security Center Web Console neu. Dazu dient der folgende Befehl:
   ```
   sudo systemctl restart KSC*
   ```

Nachdem das Upgrade erfolgreich abgeschlossen wurde, können Sie in Ihrem Browser die Adresse von Kaspersky Security Center Web Console aufrufen und sich anmelden.

Kaspersky Security Center Web Console unter Astra Linux in der geschlossenen Softwareumgebung aktualisieren

In diesem Artikel wird beschrieben, wie Sie den Server der Web Console von Kaspersky Security Center (auch "Kaspersky Security Center Web Console" genannt) unter dem Betriebssystem Astra Linux Special Edition aktualisieren.

So aktualisieren Sie Kaspersky Security Center Web Console:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center Web Console aktualisieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

2. Lesen und akzeptieren Sie den Endbenutzer-Lizenzvertrag (EULA). Wenn das Programmpaket von Kaspersky Security Center Linux keine txt-Datei mit dem Text der EULA enthält, können Sie die Datei von der Kaspersky-Website herunterladen. Wenn Sie die Bedingungen des Lizenzvertrags nicht akzeptieren, können Sie Kaspersky Security Center Web Console nicht mithilfe der Installationsdatei aktualisieren.

3. Verwenden Sie die Antwortdatei, die Sie vor der Installation von Kaspersky Security Center Web Console vorbereitet haben. Die Datei heißt "ksc-web-console-setup.json" und befindet sich unter "/etc/ksc-web-console-setup.json".

   Wenn die Antwortdatei nicht vorhanden ist, erstellen Sie eine neue Antwortdatei, in der die Parameter für die Verbindung von Kaspersky Security Center Web Console mit dem Administrationsserver enthalten sind. Geben Sie der Datei den Namen "ksc-web-console-setup.json" und speichern Sie diese anschließend im Verzeichnis "/etc".

   Beispiel für eine Antwortdatei mit den minimal notwendigen Parametern

Die Gruppe an Parametern in der Antwortdatei hängt von der Version des Administrationsservers ab, mit welcher die Kaspersky Security Center Web Console verbunden ist:

- Administrationsserver ab Version 16

  Beispiel für eine Antwortdatei mit minimalen Parametern für die Anmeldung am Administrationsserver Version 16 oder höher:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
        "Administration Server v16": {
            "iamHost": "ksc16.example.com",
            "iamOAuthPort": 4444,
            "iamProxyPort": 9050,
            "iamCertPath": "/var/opt/kaspersky/klnagent_srv/iam/main_certificate.pem",
            "iamPATPath": "/var/opt/kaspersky/klnagent_srv/iam/initial_token.txt",
            "kscPort": 13299,
            "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
        }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

- Administrationsserver Version 15.4 oder niedriger

  Beispiel für eine Antwortdatei mit minimalen Parametern für die Anmeldung am Administrationsserver Version 15.4 oder niedriger:

```
{
    "address": "ksc-web-console.example.com",
    "port": 8080,
    "trusted":  {
         "Administration Server v15.4": {
             "kscHost": "ksc.example.com",
             "kscPort": 13299,
             "kscCertPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"
         }
    },
    "certDomain":"ksc-web-console.example.com",
    "acceptEula": true
}
```

Sie können die Kaspersky Security Center Web Console entweder auf demselben Gerät, auf dem der Administrationsserver installiert ist, oder auf einem anderen Gerät installieren. Wenn die Kaspersky Security Center Web Console auf einem anderen Gerät installiert ist, unterscheidet sich die Adresse der Kaspersky Security Center Web Console (durch `address` angegeben) von der Adresse des Administrationsservers (durch `iamHost` oder `kscHost` angegeben). Wenn die Kaspersky Security Center Web Console und der Administrationsserver auf demselben Gerät installiert sind, besitzen diese Parameter die gleichen Werte.

Der Wert `iamHost` muss mit der IAM-Adresse übereinstimmen, die Sie bei der Installation des Administrationsservers angegeben haben. Um die angegebene IAM-Adresse zu erhalten, führen Sie folgenden Befehl auf dem Gerät mit dem installierten Administrationsserver aus:

```
grep "iam_address:" /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
```

Weiter Informationen dazu finden Sie in folgendem Artikel: Installationsparameter für Kaspersky Security Center Web Console.

Sie können der Liste der vertrauenswürdigen Server mehrere Administrationsserver unterschiedlicher Versionen hinzufügen. In diesem Fall können die Server unterschiedliche Authentifizierungsmethoden verwenden.

4. Stellen Sie sicher, dass in der Datei `/etc/digsig/digsig_initramfs.conf` der Parameter `DIGSIG_ELF_MODE` den folgenden Wert besitzt:

   ```
   DIGSIG_ELF_MODE=1
   ```

5. Stellen Sie sicher, dass das Kompatibilitätspaket `astra-digsig-oldkeys` installiert ist.

   Sollte das Paket nicht installiert sein, führen Sie den folgenden Befehl aus:

   ```
   apt install astra-digsig-oldkeys
   ```

6. Erstellen Sie ein Verzeichnis für den Schlüssel der Anwendung, falls noch nicht vorhanden:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. Legen Sie den Anwendungsschlüssel "/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg" in dem Verzeichnis ab, das Sie beim vorherigen Schritt erstellt haben:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > Wenn der Anwendungsschlüssel "kaspersky_astra_pub_key.gpg" nicht im Lieferumfang von Kaspersky Security Center Linux enthalten ist, können Sie den Schlüssel über den folgenden Link herunterladen: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Aktualisieren Sie die RAM-Disks:

   ```
   update-initramfs -u -k all
   ```

   Starten Sie das System neu.

9. Verwenden Sie unter einem Benutzerkonto mit Root-Rechten die Befehlszeile, um die Setup-Datei auszuführen. Die Setup-Datei können Sie von der Kaspersky-Website herunterladen.

   Um eine ältere Version von Kaspersky Security Center Web Console zu aktualisieren, führen Sie den folgenden Befehl aus:

   ```
   sudo apt-get install ksc-web-console-<Build-Nummer>.x86_64.deb
   ```

   Dadurch wird die Setup-Datei entpackt. Bitte warten Sie, bis die Installation abgeschlossen ist.

10. Starten Sie alle Dienste von Kaspersky Security Center Web Console neu. Dazu dient der folgende Befehl:

    ```
    sudo systemctl restart KSC*
    ```

Nachdem das Upgrade erfolgreich abgeschlossen wurde, können Sie in Ihrem Browser die Adresse von Kaspersky Security Center Web Console aufrufen und sich anmelden.

Migration nach Kaspersky Security Center Linux

Die Migration von Kaspersky Security Center Windows zu Kaspersky Security Center Linux ist mittels Backup der Daten des Administrationsservers (mit dem Tool "klbackup") und mittels Migrationsassistent möglich.

In der folgenden Tabelle können Sie die wichtigsten Funktionen und Einschränkungen der Migration anhand der Daten des Administrationsservers und mittels des Migrationsassistenten vergleichen. Auf diese Weise können Sie entscheiden, welcher Ansatz für Ihre Organisation der passendere ist.

Parameter	Daten-Backup des Administrationsservers	Migrationsassistent
Migrationsprozess	Erstellen eines vollständigen Backups der Daten des Administrationsservers von Kaspersky Security Center Windows und Wiederherstellen des Backups auf einem Administrationsserver von Kaspersky Security Center Linux	Auswählen und Exportieren von Daten des Administrationsservers für die Migration, Importieren dieser Daten in den Administrationsserver von Kaspersky Security Center Linux und verwaltete Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen
Merkmale der Migrationsmethode	• Migration aller Daten des Administrationsservers • Migration einer beliebigen Anzahl verwalteter Geräte • Wird verwendet, um eine vollständige Kopie des Administrationsservers von Kaspersky Security Center Windows zu erstellen und diese auf den Administrationsserver von Kaspersky Security Center Linux zu übertragen.	• Teilweise Migration der Daten des Administrationsservers • Zu migrierende Objekte können ausgewählt werden • Zu migrierende Administrationsgruppen oder Untergruppen können maximal 10.000 Geräte umfassen • Wird verwendet, um die Daten des Administrationsservers teilweise zu migrieren. Es werden nur Gruppenobjekte innerhalb des Migrationsbereichs migriert – Gruppenobjekte außerhalb des Migrationsbereichs müssen manuell wiederhergestellt werden.
Migrationsbereich	Vollständige Übertragung der Daten des Administrationsservers mit einer unbegrenzten Anzahl verwalteter Geräte	• Struktur der Administrationsgruppen • Verwaltete Geräte innerhalb von Administrationsgruppen (**max. 10.000 Geräte**) • Tags, zugewiesen an migrierende Geräte • Globale Aufgaben des Administrationsagenten und der verwalteten Anwendungen (nicht für Administrationsserver) • Gruppenaufgaben des Administrationsagenten und der verwalteten Anwendungen • Richtlinien verwalteter Anwendungen • Berichtsvorlagen • Benutzerrollen • Interne Benutzer und Sicherheitsgruppen • Benutzerdefinierte Programmkategorien mit manuell hinzugefügtem Inhalt • Benutzerdefinierte Geräteauswahlen
Nicht migrierter Bereich	—	• Globale Aufgaben des Administrationsservers • Auf dem Administrationsserver gespeicherte Ereignisse • Datenverwaltung der Programmpakete zur Remote-Installation • Zertifikat des Administrationsservers • Lizenzschlüssel, die vom Administrationsserver und von verwalteten Programmen verwendet werden • Virtuelle Administrationsserver • Richtlinieneinstellungen des Administrationsagenten • Verschiebungsregeln für Geräte • Regeln für das automatische Zuweisen von Tags an Geräte • Verteilungspunkte • Auf dem Administrationsserver gespeicherte Einstellungen von Kaspersky-Anwendungen
Unterstützte Versionen von Kaspersky Security Center	• Jede unterstützte Version von Kaspersky Security Center Windows • Kaspersky Security Center Linux Version 15.2 oder höher	• Kaspersky Security Center Windows Version 14.2 oder höher • Kaspersky Security Center Linux Version 15 oder höher
DBMSs, zwischen denen migriert werden kann	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro (nur bei Migration von Kaspersky Security Center Windows Version 14.2 oder höher mit installiertem Patch zu Kaspersky Security Center Linux Version 15.3 oder höher) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro (nur bei einer Migration von Kaspersky Security Center Windows Version 15.1 oder höher auf Kaspersky Security Center Linux Version 16 oder höher)	Uneingeschränkte Migration zwischen unterstützten DBMS

Migration auf Kaspersky Security Center Linux mittels Daten-Backup des Administrationsservers

Sie können ein Daten-Backup verwenden, um die Daten des Administrationsservers von Kaspersky Security Center Windows auf Kaspersky Security Center Linux zu migrieren. Stellen Sie vor der Migration sicher, dass die erforderlichen Funktionen von Kaspersky Security Center Windows durch Kaspersky Security Center Linux unterstützt werden.

Aus Gründen der Übersichtlichkeit ist ein Video zur Migration der Daten des Administrationsservers auf Kaspersky Security Center Linux mittels Backup verfügbar.

Einschränkungen

- Eine Migration ist zwischen den folgenden DBMS möglich:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- Wenn die Daten des Administrationsservers in einer Microsoft SQL Server-, MySQL- oder MariaDB-Datenbank gespeichert werden, wird deren Migration zu MySQL oder MariaDB von jeder unterstützten Version von Kaspersky Security Center Windows auf Kaspersky Security Center Linux Version 15.2 oder höher unterstützt.
- Die Migration von Administrationsserverdaten, die in der PostgreSQL-Datenbank gespeichert sind, zu einer anderen PostgreSQL-Datenbank oder von einer Postgres Pro-Datenbank zu Postgres Pro wird von Kaspersky Security Center Windows Version 15.1 oder höher auf Kaspersky Security Center Linux Version 16 oder höher unterstützt.
- Wenn die Daten des Administrationsservers in einer Microsoft SQL Server-Datenbank gespeichert werden, wird deren Migration zu PostgreSQL oder Postgres Pro von Kaspersky Security Center Windows Version 14.2 oder höher auf Kaspersky Security Center Linux Version 15.2 oder höher unterstützt.

  Um die Migration auf PostgreSQL oder Postgres Pro zu unterstützen, müssen Sie beim Technischen Support von Kaspersky einen der folgenden Patches anfragen und ihn anschließend installieren:
  - Für Kaspersky Security Center 14.2 Windows: 14.2.0.26967-pf5
  - Für Kaspersky Secure Mobility Management basierend auf Kaspersky Security Center 14.2 Windows: 14.2.0.48079-pf5

- Für Kaspersky Security Center 15.1 Windows: 15.1.0.20748-pf2

  Die Migration auf PostgreSQL oder Postgres Pro wird auch nach einem Update von Kaspersky Security Center Windows auf Version 15.1.0.22239 verfügbar.

- Wenn Sie MySQL oder MariaDB als DBMS für Kaspersky Security Center Windows und für Kaspersky Security Center Linux verwenden, muss der Parameter `lower_case_table_names` für das aktuelle und das neue DBMS übereinstimmen.

  Überprüfen Sie daher den Parameter `lower_case_table_names`, bevor Sie ein Daten-Backup anlegen. Wenn Sie anschließend MySQL oder MariaDB für Kaspersky Security Center Linux installieren, müssen Sie für diesen Parameter denselben Wert angeben, der unter Windows für diesen Parameter angegeben war.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, **sehen Sie sich die Anforderungen an ein benutzerdefiniertes Zertifikat an**.

Wenn Sie anstelle des selbstsignierten Zertifikats ein benutzerdefiniertes Zertifikat verwenden, müssen Sie vor dem Upgrade von Kaspersky Security Center Linux auf die neuere Version sicherstellen, dass das Zertifikat den "Subject Alternative Name" (SAN) enthält. Wenn dies nicht der Fall ist, müssen Sie das Zertifikat unbedingt vor dem Upgrade von Kaspersky Security Center Linux ersetzen. Andernfalls können Sie sich nach dem Upgrade nicht mehr in der Webkonsole anmelden.

Um sicherzustellen, dass das Zertifikat den SAN enthält:

1. Führen Sie auf dem Gerät mit dem installierten Administrationsserver folgenden Befehl aus:

   - Für ein Linux-Gerät:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout -ext subjectAltName
     ```

   - Für ein Windows-Gerät:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Stellen Sie sicher, dass der "Subject Alternative Name" in der Befehlsausgabe angezeigt wird und die Adresse des Administrationsservergeräts enthält.

3. Falls der "Subject Alternative Name" nicht angezeigt wird, verwenden Sie das Tool klsetsrvcert, um Ihr benutzerdefiniertes Zertifikat durch ein Zertifikat zu ersetzen, dass die Anforderungen erfüllt.

Schritte

Die Migration mittels Backup der Daten des Administrationsservers erfolgt schrittweise:

1. **Überprüfen, dass Sie über das interne Benutzerkonto des Administrators verfügen, mit dem Sie sich am Administrationsserver anmelden können.**

   Das Administratorkonto wird für die Anmeldung am Kaspersky Security Center Linux Administrationsserver verwendet. Wenn Sie nicht über dieses Konto verfügen und lediglich mit einem lokalen Windows-Konto oder einem Domänenkonto angemeldet sind, können Sie sich nach der Wiederherstellung des Backups nicht beim Kaspersky Security Center Linux Administrationsserver anmelden. Vom Kaspersky Security Center Linux Administrationsserver wird das Anmelden mit einem lokalen Windows-Konto nicht unterstützt. Das Anmelden mit einem Domänenkonto ist möglich, erfordert aber möglicherweise eine zusätzliche Konfiguration des Administrationsservers.

   Wenn Sie kein Administratorkonto besitzen, müssen Sie dieses Konto nach dem Wiederherstellen der Backup-Kopie mithilfe des Tools "kladduser" erstellen.

2. **Eine aktuelle Backup-Kopie der Daten des Administrationsservers von Kaspersky Security Center Windows erstellen**

   Je nachdem, welches DBMS Sie für Kaspersky Security Center Windows und Kaspersky Security Center Linux verwenden, führen Sie einen der folgenden Schritte aus:

   - Bei einer Migration von MySQL oder MariaDB auf MySQL oder MariaDB: Legen Sie eine Backup-Kopie anhand des Tools klbackup oder der Aufgabe zum Anlegen eines Daten-Backups auf dem Gerät mit dem installierten Administrationsserver an.
   - Bei einer Migration von PostgreSQL auf PostgreSQL und von PostgreSQL Pro auf PostgreSQL Pro: Erstellen Sie auf dem Gerät mit dem installierten Administrationsserver eine Backup-Kopie mittels des Tools klbackup oder der Aufgabe zum Anlegen eines Backups.
   - Bei einer Migration von Microsoft SQL Server auf MySQL oder MariaDB: Erstellen Sie ein Backup mittels des Tools klbackup mit aktivierter Option **Auf MySQL/MariaDB-Format migrieren**.
   - Bei einer Migration von Microsoft SQL Server zu PostgreSQL oder Postgres Pro:

     1. Installieren Sie den Patch für den Administrationsserver, um die Migration zu PostgreSQL und Postgres Pro zu unterstützen. Wenden Sie sich an den Technischen Support, um diesen Patch zu erhalten.

        Für Kaspersky Security Center 15.1 Windows können Sie auf die Version 15.1.0.22239 aktualisieren, anstatt den Patch zu installieren.

     2. Erstellen Sie ein Backup mittels des Tools "klbackup".

        Wenn Sie klbackup über die Befehlszeile ausführen, verwenden Sie das Flag `-migrate postgres`.

        Wenn Sie die Benutzeroberfläche von "klbackup" verwenden, aktivieren Sie die Option **Auf Postgres-Format migrieren**.

   Trennen Sie nach dem Erstellen der Backup-Kopie den Administrationsserver von Kaspersky Security Center Windows vom Netzwerk.

3. **Ein neues Gerät auf die Installation von Kaspersky Security Center Linux vorbereiten**

Führen Sie in diesem Schritt des Szenarios die folgenden Aktionen aus:

1. Wählen Sie ein neues Gerät, auf dem der Administrationsserver installiert werden soll. Dieses Gerät muss die Hard- und Softwarevoraussetzungen erfüllen. Überprüfen Sie auch, ob die auf dem Administrationsserver verwendeten Ports verfügbar sind.

2. Weisen Sie dem neuen Gerät dieselbe Adresse zu.

   Dem neuen Administrationsserver können der NetBIOS-Name, der FQDN und die statische IP-Adresse zugewiesen werden. Dies hängt davon ab, welche Adresse für den Administrationsagenten im Installationspaket des Administrationsagenten angegeben wurde, als die Administrationsagenten verteilt wurden. Alternativ können Sie die Verbindungsadresse verwenden, die den Administrationsserver bestimmt, mit dem der Administrationsagent eine Verbindung herstellt (diese Adresse kann auf verwalteten Geräten mithilfe des Tools "klnagchk" ermittelt werden).

4 DBMS installieren und konfigurieren

Führen Sie in diesem Schritt des Szenarios die folgenden Aktionen aus:

1. Wählen Sie den DBMS-Typ aus, der die optimale Leistung bietet. Berücksichtigen Sie dabei die Anzahl der vernetzten Geräte sowie die Topologie und Auslastung des Netzwerks. Sie können jedes unterstützte DBMS verwenden.

2. Installieren Sie das DBMS gemäß dem DBMS-Typ, der beim Anlegen des Backups ausgewählt wurde. Informationen zur Installation des ausgewählten DBMS finden Sie in der DBMS-Dokumentation.

   Legen Sie manuell eine Datenbank für IAM an.

   > Die neue Datenbankversion darf nicht niedriger sein als die aktuelle Version.

3. Konfigurieren Sie das DBMS für die Verwendung mit Kaspersky Security Center Linux:

- Den MariaDB x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren
- PostgreSQL- oder Postgres Pro-Server für die Ausführung mit Kaspersky Security Center Linux konfigurieren
- Den MySQL x64-Server für die Verwendung mit Kaspersky Security Center Linux konfigurieren

5 Kaspersky Security Center Linux installieren

Installieren Sie Kaspersky Security Center Linux auf dem neuen Gerät:

Das während der Installation erstellte interne Benutzerkonto des Administrators geht ebenso wie andere Objekte (Gruppen, Richtlinien, Aufgaben, Benutzer), die Sie vor der Wiederherstellung der Administrationsserverdaten aus dem Backup erstellt haben, nach der Wiederherstellung verloren. Diese Objekte werden durch Objekte ersetzt, die im Backup enthalten sind.

6 Daten des Administrationsservers aus der Backup-Kopie wiederherstellen

Führen Sie in diesem Schritt des Szenarios die folgenden Aktionen aus:

1. Stellen Sie die Daten des Administrationsservers auf dem neuen Gerät mithilfe des Tools klbackup wieder her.

   > Aufgrund von Einschränkungen von PostgreSQL müssen Sie dem Konto, das der Administrationsserver für die Verbindung mit dem DBMS verwendet, vorübergehend die Superuser-Berechtigungen für PostgreSQL erteilen.

2. Wenn Sie nicht über das interne Benutzerkonto des Administrators, mit dem Sie sich am Kaspersky Security Center Administrationsserver angemeldet haben, verfügten und Sie ein lokales Windows-Konto oder ein Domänenkonto verwendet haben, nutzen Sie das Tool "kladduser", um wie folgt ein Administratorkonto zu erstellen:

   `/opt/kaspersky/ksc64/sbin/kladduser -n kscadmin -p <Kennwort>`

   wobei der Parameter `<Kennwort>` die folgenden Anforderungen erfüllen muss:

   - Das Benutzerkennwort muss mindestens 8 Zeichen und darf maximal 256 Zeichen enthalten.
   - Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
     - Großbuchstaben (A–Z)
     - Kleinbuchstaben (a–z)
     - Ziffern (0–9)
     - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **Konfigurieren Sie die Überprüfung des Zertifikats durch Administrationsserver und IAM-Server.**

8. **Server der Web Console von Kaspersky Security Center installieren und Administrationsserver konfigurieren**

   Führen Sie in diesem Schritt des Szenarios die folgenden Aktionen aus:

   1. Installieren Sie die Kaspersky Security Center Web Console.

      Wenn die Kaspersky Security Center Web Console bereits installiert ist, installieren Sie die Web Console mit der gleichen Antwortdatei erneut.

      Melden Sie sich mit dem internen Benutzerkonto des Administrators an der Kaspersky Security Center Web Console an.

      Nach der Wiederherstellung der Daten des Administrationsservers dauert die Dateninitialisierung normalerweise bis zu 15 Minuten. Die genaue Zeit ist jedoch von der Hardwareleistung und vom Umfang der Daten des Administrationsservers abhängig. Während dieser Zeit kann die Kaspersky Security Center Web Console möglicherweise keine Verbindung herstellen und zeigt entsprechende Fehler an.

   2. Nachdem die Dateninitialisierung in der Datenbank abgeschlossen ist, überprüfen Sie die Funktionstüchtigkeit der Hauptfunktionen des Administrationsservers. Stellen Sie sicher, dass sich der Administrationsserver mit den verwalteten Geräten synchronisiert und dass die Daten des Administrationsservers wiederhergestellt wurden.

   3. Fragen Sie die Domänencontroller ab, um Informationen über die Domänenstruktur, Benutzerkonten, Sicherheitsgruppen und DNS-Namen jener Geräte wiederherzustellen, die zur Domäne gehören.

   4. Überprüfen Sie die migrierten Aufgaben. Wenn einer ihrer Parameter einen Windows-Dateipfad enthält, ersetzen Sie diesen durch den entsprechenden Linux-Dateipfad.

   5. Deinstallieren Sie bei Bedarf den Administrationsserver und den Datenbankserver vom bisherigen Gerät.

      Das Netzwerk darf nicht mehrere Administrationsserver enthalten, die sich die gleiche Verbindungsadresse und das gleiche Serverzertifikat teilen.

Der Administrator hat Zugriff auf die Daten des Administrationsservers und auf die verwalteten Geräte, die in Kaspersky Security Center Windows verfügbar waren. Dies gilt jedoch unter der Einschränkung, dass die erforderlichen Funktionen in Kaspersky Security Center Linux unterstützt werden.

Video: Migration auf Kaspersky Security Center Linux mittels Daten-Backup des Administrationsservers

Sehen Sie sich das Video an, um zu erfahren, wie Sie die Daten des Administrationsservers von Kaspersky Security Center Windows mittels Daten-Backup des Administrationsservers (mit dem Dienstprogramm klbackup) auf Kaspersky Security Center Linux migrieren.

Um die Migration auf PostgreSQL oder Postgres Pro zu unterstützen, müssen Sie beim Technischen Support von Kaspersky einen der folgenden Patches anfragen und ihn anschließend installieren:

– Für Kaspersky Security Center 14.2 Windows: 14.2.0.26967-pf5
– Für Kaspersky Secure Mobility Management basierend auf Kaspersky Security Center 14.2 Windows: 14.2.0.48079-pf5
– Für Kaspersky Security Center 15.1 Windows: 15.1.0.20748-pf2

Die Migration auf PostgreSQL oder Postgres Pro wird auch nach einem Update von Kaspersky Security Center Windows auf Version 15.1.0.22239 verfügbar.

Migration auf Kaspersky Security Center Linux mittels Daten-Backup des Administrationsservers. Video

Migration zu Kaspersky Security Center Linux mittels Migrationsassistenten

Mithilfe dieses Szenarios können Sie die Struktur der Administrationsgruppe, einschließlich verwalteter Geräte und anderer Gruppenobjekte (Richtlinien, Aufgaben, globale Aufgaben, Tags und Geräteauswahlen) aus Kaspersky Security Center Windows unter die Verwaltung von Kaspersky Security Center Linux übertragen.

Einschränkungen:

- Eine Migration ist nur von Kaspersky Security Center Windows ab Version 14.2 zu Kaspersky Security Center Linux ab Version 15 möglich.
- Dieses Szenario kann nur unter Verwendung von Kaspersky Security Center Web Console durchgeführt werden.

Bevor Sie beginnen, machen Sie sich mit den Funktionen und Einschränkungen von Kaspersky Security Center Linux vertraut:

- Funktionsunterschiede zwischen Kaspersky Security Center Windows und Kaspersky Security Center Linux
- Liste mit Kaspersky-Anwendungen, die von Kaspersky Security Center Linux unterstützt werden

Schritte

Die Migration durchläuft die die folgenden Schritte:

1. **Auswählen einer Migrationsmethode**

   Die Migration auf Kaspersky Security Center Linux erfolgt mithilfe des Migrationsassistenten. Die Schritte des Migrationsassistenten hängen davon ab, ob die Administrationsserver für Kaspersky Security Center Windows und Kaspersky Security Center Linux hierarchisch angeordnet sind:

   - Migration unter Verwendung einer Hierarchie von Administrationsservern

     Wählen Sie diese Option, wenn der Administrationsserver für Kaspersky Security Center Windows als sekundärer Administrationsserver für Kaspersky Security Center Linux fungiert. Sie verwalten den Migrationsprozess und wechseln zwischen Servern innerhalb einer einzigen Instanz der Kaspersky Security Center Web Console. Wenn Sie diese Option bevorzugen, können Sie die Administrationsserver in einer Hierarchie anordnen, um den Migrationsvorgang zu vereinfachen. Erstellen Sie dazu die Hierarchie, bevor Sie mit der Migration beginnen.

   - Migration mithilfe einer Exportdatei (zip-Archiv)

     Wählen Sie diese Option, wenn die Administrationsserver für Kaspersky Security Center Windows und Kaspersky Security Center Linux nicht in keiner Hierarchie angeordnet sind. Sie verwalten den Migrationsprozess mit zwei Instanzen der Kaspersky Security Center Web Console – eine Instanz für Kaspersky Security Center Windows und eine weitere für Kaspersky Security Center Linux. In diesem Fall verwenden Sie die Exportdatei, die Sie während des Exports aus Kaspersky Security Center Windows erstellt und heruntergeladen haben, und importieren diese Datei in Kaspersky Security Center Linux.

2. **Sichern Sie das Zertifikat und den privaten Schlüssel des Administrationsservers für Kaspersky Security Center Windows (optionaler Schritt)**

   Sie können die verwalteten Geräte unter die Verwaltung des Administrationsservers für Kaspersky Security Center Linux stellen, indem Sie das Zertifikat und den privaten Schlüssel des Administrationsservers aus einer Backup-Kopie wiederherstellen. Erstellen Sie in diesem Fall ein Backup des Zertifikats und privaten Schlüssels des Administrationsservers für Kaspersky Security Center Windows. In Schritt 6 müssen Sie dann das Zertifikat und den privaten Schlüssel wiederherstellen.

3. **Daten aus Kaspersky Security Center Windows exportieren**

   Öffnen Kaspersky Security Center Windows und starten Sie anschließend den Migrationsassistenten.

4. **Daten in Kaspersky Security Center Linux importieren**

   Fahren Sie mit dem Migrationsassistenten fort, um die exportierten Daten in Kaspersky Security Center Linux zu importieren. Wenn die Server hierarchisch angeordnet sind, wird der Import nach einem erfolgreichen Export innerhalb desselben Assistenten automatisch gestartet. Wenn die Server nicht in einer Hierarchie angeordnet sind, fahren Sie nach dem Wechsel zu Kaspersky Security Center Linux mit dem Migrationsassistenten fort.

5. **Ausführen zusätzlicher Aktionen, um Objekte und Einstellungen manuell von Kaspersky Security Center Windows nach Kaspersky Security Center Linux zu übertragen (optionaler Schritt)**

   Möglicherweise möchten Sie auch die Objekte und Einstellungen übertragen, die nicht mithilfe des Migrationsassistenten übertragen werden können. Sie können beispielsweise folgende Vorgänge zusätzlich ausführen:

   - Übertragen der Lizenzschlüssel, die vom Administrationsserver und von verwalteten Programmen verwendet werden
   - Konfigurieren der globalen Aufgaben des Administrationsservers
   - Richtlinieneinstellungen des Administrationsagenten konfigurieren
   - Installationspakete für Programme erstellen
   - Virtuelle Server erstellen
   - Regeln für das Verschieben von Geräten konfigurieren
   - Regeln für das automatische Zuweisen von Tags an Geräte konfigurieren
   - Programmkategorien erstellen
   - Verteilungspunkte zuweisen und konfigurieren

     Wenn Sie ein Gerät, das als Verteilungspunkt fungiert, auf einen anderen Administrationsserver verschieben, werden die vom Verteilungspunkt abgedeckten Geräte nicht automatisch verschoben. Sie müssen jedes Gerät einzeln verschieben. Wenn ein Verteilungspunkt als Gateway fungiert, müssen Sie das Skript `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl` ausführen, damit der Verteilungspunkt nicht mehr als Gateway dient.

6. **Die importierten verwalteten Geräte unter die Verwaltung von Kaspersky Security Center Linux verschieben**

   Um die Migration abzuschließen, verschieben Sie die importierten verwalteten Geräte unter die Verwaltung von Kaspersky Security Center Linux. Sie können dies auf eine der folgenden Arten tun:

   - Mithilfe des Tools klmover

     Verwenden Sie das Tool "klmover" und geben Sie die Verbindungseinstellungen des neuen Administrationsservers an.

   - Mittels der Aufgabe *Administrationsserver ändern*

     Erstellen Sie die Aufgabe *Administrationsserver ändern* und geben Sie dabei die importierten verwalteten Geräte, den neuen Administrationsserver und weitere Aufgabeneinstellungen an. Führen Sie anschließend die Aufgabe aus, um die verwalteten Geräte unter Verwaltung des Administrationsservers für Kaspersky Security Center Linux zu stellen.

- Durch Deinstallation (bei bereits installierten) und weitere Installation des Administrationsagenten auf den verwalteten Geräten

  Erstellen Sie ein neues Installationspaket des Administrationsagenten und geben Sie die Verbindungseinstellungen des neuen Administrationsservers in den Eigenschaften des Installationspakets an. Deinstallieren Sie den Administrationsagenten auf den importierten verwalteten Geräten und verwenden Sie anschließend das erstellte Installationspaket, um den Administrationsagenten auf den importierten verwalteten Geräten mittels einer Aufgabe zur Remote-Installation zu installieren. Sie können auch ein autonomes Installationspaket erstellen und den Administrationsagenten mittels des Pakets lokal installieren. Weitere Informationen finden Sie unter Verwaltete Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen.

- Durch das Wiederherstellen des Zertifikats und privaten Schlüssels des Administrationsservers aus einer Backup-Kopie (nur für die Migration auf Kaspersky Security Center Linux Version 15.1 oder höher).

  Weisen Sie dem Gerät mit dem Administrationsserver für Kaspersky Security Center Linux dieselbe Netzwerkadresse zu wie dem Administrationsserver für Kaspersky Security Center Windows. Führen Sie das Tool klbackupmit dem Parameter `-cert_only` aus, um das Zertifikat des Administrationsservers und den privaten Schlüssel aus der Backup-Kopie wiederherzustellen, die Sie in Schritt 2 gespeichert haben. Führen Sie in der Befehlszeile den folgenden Befehl aus: `/opt/kaspersky/ksc64/sbin/klbackup -path <Pfad zur Backup-Kopie des Administrationsserver-Zertifikats> -restore -cert_only`. Weitere Informationen dazu finden Sie unter Verwenden des klbackup-Tools, um verwaltete Geräte unter die Verwaltung eines anderen Administrationsservers zu stellen.

7. **Administrationsagent auf die neueste Version aktualisieren**

   Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center.

8. **Sicherstellen, dass die verwalteten Geräte auf dem neuen Administrationsserver sichtbar sind**

   Öffnen Sie auf dem Administrationsserver mit Kaspersky Security Center Linux die Liste der verwalteten Geräte (**Asset-Verwaltung** → **Assets (Geräte)**) und überprüfen Sie die Werte in den Spalten **Sichtbar**, **Administrationsagent ist installiert** und **Letzte Verbindung mit dem Administrationsserver**.

Weitere Methoden der Datenmigration

Neben dem Migrationsassistenten gibt es eine weitere Methode zum Übertragen Ihrer aktuellen Objekte, mit denen Sie aber nur Richtlinien und Aufgaben übertragen können:

- Exportieren Sie die Aufgaben aus Kaspersky Security Center Windows und importieren Sie die Aufgaben anschließend in Kaspersky Security Center Linux.

- Exportieren Sie bestimmte Richtlinien aus Kaspersky Security Center Windows und importieren Sie die Richtlinien anschließend in Kaspersky Security Center Linux. Die zugehörigen Richtlinienprofile werden zusammen mit den ausgewählten Richtlinien exportiert und importiert.

Gruppenobjekte aus Kaspersky Security Center Windows exportieren

Für die Migration der Struktur der Administrationsgruppe einschließlich verwalteter Geräte und anderer Gruppenobjekte von Kaspersky Security Center Windows auf Kaspersky Security Center Linux müssen Sie zuerst die Daten für den Export auswählen und eine Exportdatei erstellen. Die Exportdatei enthält Informationen über alle Gruppenobjekte, die Sie migrieren möchten. Die Exportdatei wird für den anschließenden Import in Kaspersky Security Center Linux verwendet.

Sie können die folgenden Objekte exportieren:

- Aufgaben und Richtlinien verwalteter Anwendungen
- Globale Aufgaben
- Benutzerdefinierte Geräteauswahlen
- Strukturen von Administrationsgruppen und darin enthaltene Geräte
- Tags, die den zu migrierenden Geräten zugewiesen wurden

Bevor Sie mit dem Export beginnen, machen Sie sich mit den allgemeinen Informationen zur Migration auf Kaspersky Security Center Linux vertraut. Wählen Sie die Migrationsmethode – mit oder ohne Verwendung der Hierarchie der Administrationsserver für Kaspersky Security Center Windows und Kaspersky Security Center Linux.

So exportieren Sie verwaltete Geräte und zugehörige Gruppenobjekte über den Migrationsassistenten:

1. Je nachdem, ob sich der Administrationsserver für Kaspersky Security Center Windows und Kaspersky Security Center Linux in einer Hierarchie befinden, führen Sie einen der folgenden Schritte aus:
   - Wenn sich die Server in einer Hierarchie befinden, öffnen Sie die Kaspersky Security Center Web Console und wechseln Sie anschließend zum Server von Kaspersky Security Center Windows.
   - Wenn sich die Server nicht in einer Hierarchie befinden, öffnen Sie die Kaspersky Security Center Web Console, die mit Kaspersky Security Center Windows verbunden ist.
2. Gehen Sie im Hauptmenü zu **Vorgänge** → **Migration**.
3. Wählen Sie **Zu Kaspersky Security Center Linux oder auf die Open Single Management Platform migrieren**, um den Assistenten zu starten und seinen Schritten zu folgen.
4. Wählen Sie die Administrationsgruppe oder Untergruppe aus, die Sie exportieren möchten. Bitte stellen Sie sicher, dass die ausgewählte Administrationsgruppe oder Untergruppe nicht mehr als 10.000 Geräte umfasst.
5. Wählen Sie die verwalteten Anwendungen aus, deren Aufgaben und Richtlinien exportiert werden. Wählen Sie nur Anwendungen aus, die auch von Kaspersky Security Center Linux unterstützt werden. Die Objekte von nicht unterstützten Anwendungen werden zwar auch exportiert, sind aber nicht nutzbar.
6. Verwenden Sie die Links auf der linken Seite, um die globalen Aufgaben, die Geräteauswahlen und die zu exportierenden Berichte auszuwählen. Mit dem Link **Gruppenobjekte** können Sie folgende Objekte vom Export ausschließen: benutzerdefinierte Rollen, interne Benutzer und Sicherheitsgruppen sowie benutzerdefinierte Programmkategorien.

Die Exportdatei (zip-Archiv) wird erstellt. Abhängig davon, ob Sie die Migration mit Unterstützung der Hierarchie der Administrationsserver durchführen oder nicht, wird die Exportdatei wie folgt gespeichert:

- Wenn die Server in einer Hierarchie angeordnet sind, wird die Exportdatei im temporären Ordner des Servers der Web Console von Kaspersky Security Center gespeichert.
- Wenn die Server nicht in einer Hierarchie angeordnet sind, wird die Exportdatei auf Ihr Gerät heruntergeladen.

Bei einer Migration mit Unterstützung der Hierarchie der Administrationsserver startet der Import automatisch nach einem erfolgreichen Export. Für die Migration ohne Unterstützung der Hierarchie der Administrationsserver können Sie die gespeicherte Exportdatei manuell in Kaspersky Security Center Linux importieren.

Importieren der Exportdatei in Kaspersky Security Center Linux

Um aus Kaspersky Security Center Windows exportierte Informationen zu verwalteten Geräten und Objekten mitsamt deren Einstellungen zu übertragen, müssen Sie diese in Kaspersky Security Center Linux oder Kaspersky Next XDR Expert importieren.

So importieren Sie verwaltete Geräte und zugehörige Gruppenobjekte über den Migrationsassistenten:

1. Je nachdem, ob sich Administrationsserver von Kaspersky Security Center Windows und Kaspersky Security Center Linux in einer Hierarchie befinden, führen Sie einen der folgenden Schritte aus:

   - Wenn die Server in einer Hierarchie angeordnet sind, fahren Sie nach Abschluss des Exports mit dem nächsten Schritt des Migrationsassistenten fort. Der Import wird nach einem erfolgreichen Export innerhalb dieses Assistenten automatisch gestartet (siehe Schritt 2 dieser Anleitung).

   - Wenn die Server in keiner Hierarchie angeordnet sind:

     a. Öffnen Sie die Kaspersky Security Center Web Console, die mit Kaspersky Security Center Linux oder Kaspersky Next XDR Export verbunden ist.

     b. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Migration**.

     c. Wählen Sie die Exportdatei (zip-Archiv) aus, die Sie während des Exports aus Kaspersky Security Center Windows erstellt und heruntergeladen haben. Das Hochladen der Exportdatei wird gestartet.

2. Nachdem die Exportdatei erfolgreich hochgeladen wurde, können Sie den Import fortsetzen. Wenn Sie eine andere Exportdatei angeben möchten, klicken Sie auf den Link **Ändern** und wählen Sie die gewünschte Datei aus.

3. Es wird die gesamte Hierarchie der Administrationsgruppen von Kaspersky Security Center Linux wird angezeigt.

   Aktivieren Sie das Kontrollkästchen neben der Ziel-Administrationsgruppe, für welche die Objekte der exportierten Administrationsgruppe (verwaltete Geräte, Richtlinien, Aufgaben und weitere Gruppenobjekte) wiederhergestellt werden sollen.

4. Der Import der Gruppenobjekte wird gestartet. Sie können den Migrationsassistenten während des Imports nicht minimieren und keine gleichzeitigen Vorgänge ausführen. Warten Sie, bis alle Aktualisierungssymbole (🔄) neben den Elementen der Objektliste durch grüne Häkchen (✓) ersetzt wurden und der Import beendet ist.

5. Nach Abschluss des Imports wird die exportierte Struktur der Administrationsgruppen einschließlich der Gerätedetails unter der von Ihnen ausgewählten Ziel-Administrationsgruppe angezeigt. Wenn der Name des wiederherzustellenden Objekts mit dem Namen eines bereits vorhandenen Objekts identisch ist, besitzt das wiederhergestellte Objekt ein inkrementelles Suffix.

Wenn in einer migrierten Aufgabe die Details des Benutzerkontos angegeben sind, mit dem die Aufgabe ausgeführt wird, müssen Sie die Aufgabe öffnen und das Kennwort nach Abschluss des Imports erneut eingeben.

Wenn der Import mit einem Fehler abgeschlossen wurde, können Sie eine der folgenden Maßnahmen ergreifen:

- Für eine Migration mit unterstützter Hierarchie des Administrationsservers können Sie den Import der Exportdatei erneut starten.
- Für eine Migration ohne unterstützte Hierarchie des Administrationsservers können Sie den Migrationsassistenten starten, um eine andere Exportdatei auszuwählen und anschließend erneut zu importieren.

Sie können kontrollieren, ob die im Exportbereich enthaltenen Gruppenobjekte erfolgreich in Kaspersky Security Center Linux importiert wurden. Wechseln Sie dazu in den Abschnitt **Asset-Verwaltung** und stellen Sie sicher, dass die importierten Objekte in den entsprechenden Unterabschnitten erscheinen.

Beachten Sie, dass die importierten verwalteten Geräte im Unterabschnitt **Verwaltete Geräte** zwar angezeigt werden, aber weder im Netzwerk sichtbar sind, noch dass der Administrationsagent auf ihnen installiert ist und ausgeführt wird (in den folgenden Spalten steht der Wert *Nein*: **Sichtbar**, **Administrationsagent ist installiert** und **Administrationsagent wird ausgeführt**).

Um die Migration abzuschließen, müssen Sie die verwalteten Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen.

Verwaltete Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen

Nach dem in Kaspersky Security Center Linux die Informationen über verwaltete Geräte, Objekte und deren Einstellungen erfolgreich importiert wurden, müssen Sie die verwalteten Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen, um die Migration abzuschließen.

Sie können die verwalteten Geräte auf eine der folgenden Arten unter die Verwaltung von Kaspersky Security Center Linux verschieben:

- Mittels des Tools klmover.
- Mittels der Aufgabe *Administrationsserver ändern*.
- Mittels der Wiederherstellung des Zertifikats und privaten Schlüssels des Administrationsservers aus einer Backup-Kopie (nur für die Migration auf Kaspersky Security Center Linux 15.1 oder höher).

  Weitere Informationen dazu finden Sie in Stufe 6 des Hauptszenarios für die Migration.
- Mittels der Aufgabe zur Remote-Installation durchgeführten Installation des Administrationsagenten auf dem verwalteten Gerät.

So stellen Sie die verwalteten Geräte mithilfe der Installation des Administrationsagenten unter Verwaltung von Kaspersky Security Center Linux:

1. Entfernen Sie den Administrationsagenten auf den importierten verwalteten Geräten, die unter die Verwaltung von Kaspersky Security Center Linux gestellt werden sollen.
2. Wechseln Sie zum Administrationsserver für Kaspersky Security Center Windows.
3. Gehen Sie zu **Software-Verwaltung** → **Installationspakete** und öffnen Sie die Eigenschaften eines existierenden Pakets des Administrationsagenten.

Wenn in der Paketliste kein Installationspaket eines Administrationsagenten vorhanden ist laden Sie ein neues herunter.

Sie können auch ein autonomes Installationspaket erstellen und den Administrationsagenten mittels des Pakets lokal installieren.

4. Wählen Sie auf der Registerkarte **Einstellungen** den Abschnitt **Verbindung**. Geben Sie die Verbindungseinstellungen des Administrationsservers für Kaspersky Security Center Linux an.

5. Erstellen Sie eine Aufgabe zur Remote-Installation für importierte verwaltete Geräte und geben Sie anschließend das neu konfigurierte Installationspaket des Administrationsagenten an.

   Sie können den Administrationsagenten entweder über den Administrationsserver für Kaspersky Security Center Windows oder über ein Windows-Gerät installieren, das als Verteilungspunkt fungiert. Wenn Sie den Administrationsserver verwenden, aktivieren Sie die Option **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**. Wenn Sie einen Verteilungspunkt verwenden, aktivieren Sie die Option **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**.

6. Starten Sie die Aufgabe zur Remote-Installation des Programms.

Nachdem die Aufgabe zur Remote-Installation erfolgreich abgeschlossen wurde, wechseln Sie zum Administrationsserver für Kaspersky Security Center Linux und stellen Sie sicher, dass die verwalteten Geräte im Netzwerk sichtbar sind und dass der Administrationsagent auf ihnen installiert ist und ausgeführt wird (in folgenden Spalten muss der Wert auf *Ja* stehen: **Sichtbar**, **Administrationsagent ist installiert** und **Administrationsagent wird ausgeführt**).

Konfigurieren des Administrationsservers

Dieser Abschnitt beschreibt den Konfigurationsprozess und die Eigenschaften des Kaspersky Security Center Administrationsservers.

Verbindungsadresse des Administrationsservers konfigurieren

Die Verbindungsadresse des Administrationsservers wird für die folgenden Zwecke als Netzwerkadresse verwendet:

- Als Standardadresse beim Erstellen der Installationspakete des Administrationsagenten

  Nach der Installation des Administrationsagenten stellen die verwalteten Geräte mit dieser Adresse die Verbindung zum Administrationsserver her.

- Als Adresse des KSN-Proxyservers

  Die verwalteten Geräte stellen mit dieser Adresse die Verbindung zum KSN-Proxyserver her.

So konfigurieren Sie die Verbindungsadresse des Administrationsservers:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Allgemein** aus.

3. Geben Sie im neuen Fenster die neue Verbindungsadresse des Administrationsservers im Feld **Verbindungsadresse des Administrationsservers** ein.

   Die maximale Länge der Verbindungsadresse beträgt 255 Zeichen.

   Sie können den NetBIOS-Namen, den FQDN oder die IP-Adresse des Administrationsservers als Verbindungsadresse des Administrationsservers angeben.

4. Klicken Sie auf **Speichern**.

Die angegebene Adresse wird als Adresse des Administrationsservers und des KSN-Proxyservers verwendet.

Verbindung zwischen Kaspersky Security Center Web Console und Administrationsserver anpassen

Die Verbindung von Kaspersky Security Center Web Console mit dem Administrationsserver können Sie in den Eigenschaften des Administrationsservers oder in den Einstellungen der Richtlinie des Administrationsservers anpassen.

So legen Sie die Verbindungsports über die Einstellungen des Administrationsservers fest:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verbindungsports** aus.

3. Geben Sie bei Bedarf die Einstellung **SSL-Port der Web Console** an oder legen Sie andere Ports für die Verbindung des Administrationsservers fest.

Die wichtigsten Verbindungseinstellungen des ausgewählten Servers sind angegeben.

So legen Sie die Verbindungsports über die Einstellungen der Richtlinie des Administrationsservers fest:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

2. Klicken Sie auf den Namen der Richtlinie des Administrationsservers und wechseln Sie anschließend zur Registerkarte **Anwendungseinstellungen**.

3. Geben Sie bei Bedarf die Einstellung **SSL-Port der Web Console** an oder legen Sie andere Ports für die Verbindung des Administrationsservers fest.

   Wenn Sie die Option **Port für die Web Console öffnen** deaktivieren und diese Richtlinieneinstellung auf das Gerät angewendet wird, können Sie mithilfe der Kaspersky Security Center Web Console keine Verbindung zum Administrationsserver herstellen. In diesem Fall wird die Verbindung beendet. Wenn Sie einen Administrationsserver ausführen, auf den diese Richtlinie nicht angewendet wird, können Sie über die Kaspersky Security Center Web Console erneut eine Verbindung zu diesem Administrationsserver herstellen.

Die wichtigsten Verbindungseinstellungen des ausgewählten Servers sind angegeben.

Allow-Liste mit IP-Adressen für die Verbindung mit Kaspersky Security Center Linux konfigurieren

Standardmäßig sind Verbindungen mit Kaspersky Security Center Linux von allen Geräten aus zulässig. So können Sie beispielsweise den Server der Web Console von Kaspersky Security Center auf jedem Gerät installieren, dass die Voraussetzungen erfüllt. Anschließend wird sich der Server der Web Console von Kaspersky Security Center mit Kaspersky Security Center Linux verbinden. Sie können den Administrationsserver jedoch sie konfigurieren, dass nur jene Verbindungen erlaubt sind, die von den IP-Adressen ausgehen, die Sie angegeben haben. In diesem Fall werden Anmeldeversuche an Kaspersky Security Center abgelehnt, wenn etwa eine angreifende Person versucht, sich mittels eines Servers der Web Console von Kaspersky Security Center, der auf einem Gerät installiert ist, dessen IP-Adresse nicht in der Allow-Liste enthalten ist, mit Kaspersky Security Center Linux zu verbinden.

Die IP-Adresse wird überprüft, wenn sich ein Benutzer an Kaspersky Security Center Linux anmeldet oder eine Anwendung ausführt, die mit dem Administrationsserver über Kaspersky Security Center Linux-OpenAPI interagiert. In so einem Moment versucht eine Anwendung auf einem Gerät, eine Verbindung mit dem Administrationsserver herzustellen. Befindet sich die IP-Adresse des Geräts nicht auf der Allow-Liste, tritt ein Authentifizierungsfehler auf und das Ereignis KLAUD_EV_SERVERCONNECT benachrichtigt Sie darüber, dass eine Verbindung mit dem Administrationsserver abgelehnt wurde.

Anforderungen an eine Allow-Liste mit IP-Adressen

IP-Adressen werden nur überprüft, wenn die folgenden Anwendungen versuchen, sich mit dem Administrationsserver zu verbinden:

- Server der Web Console von Kaspersky Security Center

  Wenn Sie sich über die Kaspersky Security Center Web Console bei Kaspersky Security Center Linux anmelden, können Sie mit den Standardwerkzeugen des Betriebssystems eine Firewall auf dem Gerät konfigurieren, auf dem der Server der Web Console von Kaspersky Security Center installiert ist. Wenn anschließend jemand versucht, sich von einem Gerät aus an Kaspersky Security Center Linux anzumelden, wobei der Server der Web Console von Kaspersky Security Center auf einem anderen Gerät installiert ist, hilft eine Firewall, die Eindringlinge abzuweisen.

- Anwendungen, die mittels klakaut-Automatisierungsobjekten mit dem Administrationsserver interagieren

- Anwendungen, die mittels OpenAPI mit dem Administrationsserver interagieren, z. B. Kaspersky Anti Targeted Attack Platform oder Kaspersky Security for Virtualization

Geben Sie daher Adressen der Geräte an, auf denen die oben aufgeführten Anwendungen installiert sind.

Sie können sowohl IPv4- als auch IPv6-Adressen angeben. Sie können keine IP-Adressbereiche angeben.

So erstellen Sie eine Allow-Liste mit IP-Adressen

Wenn Sie zuvor noch keine Allow-Liste erstellt haben, folgen Sie den nachstehenden Anweisungen.

So erstellen Sie die Allow-Liste mit IP-Adressen zur Anmeldung an Kaspersky Security Center Linux:

1. Führen Sie auf dem Gerät des Administrationsservers die Eingabeaufforderung unter einem Konto mit Administratorrechten aus.

2. Ändern Sie das aktuelle Verzeichnis des Installationsordners von Kaspersky Security Center Linux (üblicherweise /opt/kaspersky/ksc64/sbin).

3. Geben Sie unter dem Benutzerkonto mit Root-Rechten den folgenden Befehl ein:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP-Adressen>" -t s`

   Geben Sie IP-Adressen an, die den oben aufgeführten Anforderungen entsprechen. Mehrere IP-Adressen müssen durch ein Semikolon getrennt werden.

   Beispiel, um nur einem Gerät die Verbindung mit dem Administrationsserver zu erlauben:

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s
   ```

   Beispiel, um mehreren Geräten die Verbindung mit dem Administrationsserver zu erlauben:

   ```
   klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s
   ```

4. Starten Sie den Dienst des Administrationsservers neu.

Dem Syslog-Ereignisprotokoll auf dem Administrationsserver können Sie entnehmen, ob Sie die Allow-Liste mit IP-Adressen erfolgreich konfiguriert haben.

So ändern Sie eine Allow-Liste mit IP-Adressen

Sie können eine Allow-Liste auf gleiche Weise ändern, wie Sie es bei der erstmaligen Erstellung getan haben. Führen Sie daher denselben Befehl aus und geben Sie eine neue Allow-Liste an:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<IP-Adressen>"
-t s
```

Wenn Sie einige IP-Adressen aus der Allow-Liste löschen möchten, erstellen Sie diese neu. Ihre Allow-Liste enthält beispielsweise die folgenden IP-Adressen: 192.0.2.0; 198.51.100.0 und 203.0.113.0. Sie möchten die IP-Adresse 198.51.100.0 aus der Liste löschen. Geben Sie dafür den folgenden Befehl in die Eingabeaufforderung ein:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0;
203.0.113.0" -t s
```

Stellen Sie sicher, den Dienst des Administrationsservers neu zu starten.

Zurücksetzen einer konfigurierten Allow-Liste mit IP-Adressen

So setzen Sie eine bereits konfigurierte Allow-Liste mit IP-Adressen zurück:

1. Geben Sie in der Eingabeaufforderung den folgenden Befehl unter einem Benutzerkonto mit Root-Rechten ein:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. Starten Sie den Dienst des Administrationsservers neu.

Anschließend werden IP-Adressen nicht mehr überprüft.

Die Internetzugriffseinstellungen für den Administrationsserver konfigurieren

Sie müssen den Internetzugang anpassen, um Kaspersky Security Network zu verwenden und um Updates für die Antiviren-Datenbanken von Kaspersky Security Center Linux und die verwalteten Kaspersky-Anwendungen herunterzuladen.

So geben Sie die Internetzugriffseinstellungen für den Administrationsserver an:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Konfiguration des Internetzugriffs** aus.

3. Aktivieren Sie die Option **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung benutzen wollen. Wenn die Option aktiviert ist, sind die Eingabefelder der Einstellungen verfügbar. Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:

   - **Adresse**

     Die Proxyserver-Adresse für die Verbindung von Kaspersky Security Center Linux mit dem Internet.

- **Port**

  Nummer des Ports, über den die Proxy-Verbindung zu Kaspersky Security Center Linux hergestellt wird.

- **Proxyserver für lokale Adressen umgehen**

  Bei der Verbindung mit den Geräten im lokalen Netzwerk wird kein Proxyserver verwendet.

- **Authentifizierung am Proxyserver**

  Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

  Die Eingabefelder sind verfügbar, wenn das Kontrollkästchen **Proxyserver verwenden** aktiviert ist.

- **Benutzername**

  Benutzerkonto, unter dem die Verbindung zum Proxyserver hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

- **Kennwort**

  Kennwort, das von dem Benutzer festgelegt wird, unter dessen Benutzerkonto die Proxyserver-Verbindung hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

  Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie diese für die erforderliche Zeitspanne gedrückt.

Sie können den Internetzugang auch unter Verwendung des Schnellstartassistenten konfigurieren.

Hierarchie des Administrationsservers

Einige Kundenunternehmen wie MSPs betreiben möglicherweise mehrere Administrationsserver. Die Verwaltung mehrerer vereinzelter Administrationsserver ist unpraktisch, deshalb es ist zweckmäßig, sie in einer Hierarchie zusammenzufassen. In einer Hierarchie kann ein Linux-basierter Administrationsserver sowohl als primärer Server als auch als sekundärer Server fungieren. Der primäre Linux-basierte Server kann sowohl Linux-basierte als auch Windows-basierte sekundäre Server verwalten. Ein primärer Server auf Windows-Basis kann einen sekundären Server auf Linux-Basis verwalten.

Eine "Primär/Sekundär"-Konfiguration für zwei Administrationsserver bietet die folgenden Möglichkeiten:

- Der sekundäre Administrationsserver erbt vom primären Administrationsserver die Richtlinien Aufgaben, Benutzerrollen und Installationspakete, wobei duplizierte Einstellungen entfernt werden.
- Die Geräteauswahlen auf dem primären Administrationsserver können Geräte der sekundären Administrationsserver einschließen.
- Die Berichte auf dem primären Administrationsserver können Daten (einschließlich ausführlicher Informationen) der sekundären Administrationsserver einschließen.
- Als Update-Quelle für einen sekundären Administrationsserver kann ein primärer Administrationsserver verwendet werden.

Der primäre Administrationsserver empfängt Daten von sekundären, nicht-virtuellen Administrationsservern nur im Rahmen der oben aufgeführten Optionen. Diese Einschränkung gilt nicht für virtuelle Administrationsserver, welche die Datenbank mit ihrem primären Administrationsserver teilen.

Die Hierarchie der Administrationsserver unterstützt den Mandantenfähigkeitsmodus. Dieser Modus ermöglicht es einem Hauptadministrator, mehrere Clients unabhängig voneinander zentral zu verwalten. Jedes Kundenunternehmen oder Büro ist von anderen isoliert und wird als Mandant bezeichnet. Sie können einem Mandanten mehrere verwaltete Geräte mit den dazugehörigen Daten, Einstellungen, Richtlinien und Aufgaben zuweisen und die Benutzerrechte nach Mandanten konfigurieren.

Ein primärer Administrationsserver, der in der Hauptinfrastruktur des Unternehmens installiert ist, fungiert als primärer Mandant. Der primäre Administrationsserver ermöglicht es sekundären oder virtuellen Administrationsservern – seinen isolierten Mandanten –, selbstständig ihre eigenen Ereignisse zu empfangen und zu verarbeiten und mit ihren eigenen Ressourcen, Diensten und Konfigurationen zu arbeiten.

Ein Dienstanbieter mit mehreren Kundenunternehmen kann die Funktionalität von Kaspersky Security Center Linux einschließlich der Aggregation von Alarmen und Reaktionsmaßnahmen für jedes Kundenunternehmen unabhängig voneinander bereitstellen. Zu diesem Zweck verbindet der Dienstanbieter sekundäre oder virtuelle Administrationsserver als Mandanten für jedes Kundenunternehmen. Der Dienstanbieter stellt Dienste unter Verwendung seines eigenen Personals und seiner eigenen Ressourcen bereit.

Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen

In einer Hierarchie kann ein Linux-basierter Administrationsserver sowohl als primärer Server als auch als sekundärer Server fungieren. Der primäre Linux-basierte Server kann sowohl Linux-basierte als auch Windows-basierte sekundäre Server verwalten. Ein primärer Server auf Windows-Basis kann einen sekundären Server auf Linux-Basis verwalten.

Sekundären Administrationsserver hinzufügen (Ausführung auf dem zukünftigen primären Administrationsserver)

Sie können einen Administrationsserver als sekundären Administrationsserver hinzufügen und so eine Hierarchie vom Typ "primärer/sekundärer" festlegen.

Um einen sekundären Administrationsserver hinzuzufügen, der mit Kaspersky Security Center Web Console verbunden werden kann, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Port 13000 des zukünftigen primären Administrationsservers für die Annahme von Verbindungen von sekundären Administrationsservern verfügbar ist.

2. Wechseln Sie zu den Eigenschaften des zukünftigen primären Administrationsservers:

   a. Wählen Sie im Hauptmenü einen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**), und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

   b. Bewegen Sie im neuen Navigationsbereich den Mauszeiger über den Namen des erforderlichen Administrationsservers und klicken Sie anschließend auf das Einstellungssymbol (⚙).

      Alternativ können Sie auf den Namen des Administrationsservers klicken und wenn der Name anschließend im Hauptmenü angezeigt wird, auf diesen klicken, um das Eigenschaftsfenster des Servers zu öffnen.

3. Klicken Sie im neuen Eigenschaftsfenster auf die Registerkarte **Administrationsserver**.

4. Wählen Sie das Kontrollkästchen neben der Administrationsgruppe aus, zu der Sie den virtuellen Administrationsserver hinzufügen möchten.

5. Klicken Sie in der Menüleiste auf **Sekundären Administrationsserver verbinden**.

   Der Assistent für das Hinzufügen eines sekundären Administrationsservers wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

6. Füllen Sie die folgenden Felder aus:

   - **Anzeigename des sekundären Administrationsservers**

     Ein Name, unter dem der sekundäre Administrationsserver in der Hierarchie angezeigt werden soll. Wenn Sie möchten, können Sie als Name die IP-Adresse oder einen Benutzernamen wie "Sekundärer Server für Gruppe 1" angeben.

   - **Adresse des sekundären Administrationsservers (optional)**

     Geben Sie die IP-Adresse oder den Domänennamen des sekundären Administrationsservers an.

     Dieser Parameter ist erforderlich, wenn die Option **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden** aktiviert ist.

   - **SSL-Port des Administrationsservers**

     Geben Sie die Nummer des SSL-Ports auf dem primären Administrationsserver an. Standardmäßig wird Portnummer 13000 verwendet.

   - **API-Port des Administrationsservers**

     Geben Sie die Nummer des Ports auf dem primären Aministrationsserver an, über den Verbindungen über OpenAPI eingehen sollen. Standardmäßig wird Portnummer 13299 verwendet.

   - **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden**

     Wählen Sie diese Option, wenn sich der sekundäre Administrationsserver in einer demilitarisierten Zone (DMZ) befindet.

     Wenn diese Option ausgewählt ist, initiiert der primäre Administrationsserver die Verbindung mit dem sekundären Administrationsserver. Andernfalls verbindet sich der sekundäre Administrationsserver mit dem primären Administrationsserver.

   - **Proxyserver verwenden**

     Wählen Sie diese Option, wenn die Verbindung zum sekundären Administrationsserver über einen Proxyserver hergestellt wird.

     In diesem Fall müssen Sie außerdem die folgenden Einstellungen des Proxyservers angeben:

     - **Proxyserver-Adresse**
     - **Benutzername**
     - **Kennwort**

7. Legen Sie die Verbindungseinstellungen fest:

   - Geben Sie die Adresse des zukünftigen primären Administrationsservers ein.
   - Wenn der zukünftige sekundäre Administrationsserver einen Proxyserver verwendet, geben Sie die Adresse des Proxyservers und die Anmeldeinformationen des Benutzers ein, um sich mit dem Proxyserver zu verbinden.

8. Geben Sie die Zugangsdaten des Benutzers ein, der Zugriffsrechte auf den zukünftigen sekundären Administrationsserver hat.

   Wenn die Verbindungseinstellungen korrekt sind, wird die Verbindung mit dem zukünftigen sekundären Server hergestellt und die "primär/sekundär"-Hierarchie gebildet. Wenn die Verbindung fehlgeschlagen ist, überprüfen Sie die Verbindungseinstellungen oder geben Sie das Zertifikat des zukünftigen sekundären Servers manuell an.

   Die Verbindung kann auch fehlschlagen, weil der zukünftige sekundäre Server mit einem selbstsignierten Zertifikat authentifiziert wird, das von Kaspersky Security Center Linux automatisch generiert wurde. Infolgedessen blockiert der Browser möglicherweise das Herunterladen des selbstsignierten Zertifikats. Wenn dieser Fall eintritt, können Sie Folgendes tun:

- Erstellen Sie für den zukünftigen Server ein Zertifikat, das in Ihrer Infrastruktur vertrauenswürdig ist und das die Anforderungen an benutzerdefinierte Zertifikate erfüllt.
- Fügen Sie das selbstsignierte Zertifikat des zukünftigen sekundären Servers der Liste mit vertrauenswürdigen Zertifikaten des Browsers hinzu. Es wird empfohlen, dass Sie diese Option nur verwenden, wenn Sie kein benutzerdefiniertes Zertifikat erstellen können. Informationen zum Hinzufügen eines Zertifikats zur Liste der vertrauenswürdigen Zertifikate finden Sie in der Dokumentation Ihres Browsers.

Nach Abschluss des Assistenten wird eine "primärer/sekundär"-Hierarchie gebildet. Die Verbindung zwischen dem primären und dem sekundären Administrationsserver wird über Port 13000 hergestellt. Die vom primären Administrationsserver bereitgestellten Aufgaben und Richtlinien werden abgerufen und angewendet. Der sekundäre Administrationsserver wird auf dem primären Administrationsserver in der Administrationsgruppe angezeigt, in der er hinzugefügt wurde.

Sekundären Administrationsserver hinzufügen (Ausführung auf dem zukünftigen sekundären Administrationsserver)

Wenn Sie keine Verbindung zum zukünftigen sekundären Administrationsserver aufbauen konnten (da dieser z. B. vorübergehend getrennt oder nicht verfügbar war, oder weil das Zertifikat des Administrationsservers selbstsigniert ist), können Sie trotzdem einen sekundären Administrationsserver hinzufügen.

Um einen Administrationsserver, der nicht für die Verbindung über Kaspersky Security Center Web Console verfügbar ist, als sekundären Server hinzuzufügen, gehen Sie wie folgt vor:

1. Senden Sie die Zertifikatsdatei des zukünftigen primären Administrationsservers an den Systemadministrator des Büros, in dem sich der zukünftige sekundäre Administrationsserver befindet (Sie können die Datei z. B. auf einem externen Gerät wie einem Flash-Laufwerk speichern oder per E-Mail senden).

   Die Zertifikatsdatei befindet sich auf dem zukünftigen primären Administrationsserver unter /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Bitten Sie den Systemadministrator, der für den zukünftigen sekundären Administrationsserver zuständig ist, wie folgt vorzugehen:

   a. Klicken Sie auf den Namen des Administrationsservers.

   b. Wechseln Sie auf der nächsten Seite mit Eigenschaften zum Abschnitt **Hierarchie der Administrationsserver** auf der Registerkarte **Allgemein**.

   c. Wählen Sie die Option **Dieser Administrationsserver ist in der Server-Hierarchie sekundär** aus.

   d. Geben Sie im Feld **Adresse des primären Administrationsservers** den Netzwerknamen des zukünftigen primären Administrationsservers an.

   e. Wählen Sie die zuvor gespeicherte Zertifikatsdatei des zukünftigen primären Administrationsservers aus, indem Sie auf **Durchsuchen** klicken.

   f. Aktivieren Sie bei Bedarf das Kontrollkästchen **Primären Administrationsserver mit sekundärem Administrationsserver in der DMZ verbinden**.

   g. Wenn die Verbindung mit dem zukünftigen primären Administrationsserver über einen Proxyserver hergestellt wird, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und geben Sie die Verbindungseinstellungen ein.

   h. Klicken Sie auf die Schaltfläche **Speichern**.

Die "primär/sekundär"-Hierarchie wird gebildet. Der primäre Administrationsserver nimmt über Port 13000 Verbindungen vom sekundären Administrationsserver an. Die vom primären Administrationsserver bereitgestellten Aufgaben und Richtlinien werden abgerufen und angewendet. Der sekundäre Administrationsserver wird auf dem primären Administrationsserver in der Administrationsgruppe angezeigt, in der er hinzugefügt wurde.

Liste mit sekundären Administrationsservern anzeigen

So zeigen Sie eine Liste mit sekundären (einschl. virtuellen) Administrationsservern an:

1. Wählen Sie im Hauptmenü einen beliebigen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**).

2. Klicken Sie im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

Im neuen Navigationsbereich wird die Liste der sekundären (einschließlich virtueller) Administrationsserver angezeigt. Sie können auf den Namen eines dieser Administrationsserver klicken, um zu ihm zu wechseln.

Sie können nicht zu virtuellen Administrationsservern wechseln, wenn Sie den Navigationsbereich über die Abschnitte **IP-Bereiche** und **Gelöschte Objekte** geöffnet haben.
Die Administrationsgruppen werden ebenfalls angezeigt. Die Gruppen stehen zur Verwaltung zur Verfügung, wenn Sie den Navigationsbereich über einen der folgenden Abschnitte geöffnet haben: **Assets (Geräte)**, **Richtlinien**, **Aufgaben** und **Verteilungspunkte**. Andernfalls sind die Gruppen ausgegraut.

Wenn Sie in der Kaspersky Security Center Web Console mit Ihrem primären Administrationsserver verbunden sind und keine Verbindung zu einem virtuellen Administrationsserver, der von einem sekundären Administrationsserver verwaltet wird, herstellen können, haben Sie folgende Möglichkeiten:

- **Ändern Sie die vorhandene Installation von Kaspersky Security Center Web Console, um den sekundären Server zur Liste der vertrauenswürdigen Administrationsserver hinzuzufügen.** Anschließend können Sie sich in Kaspersky Security Center Web Console mit dem virtuellen Administrationsserver verbinden.

  1. Führen Sie unter einem Konto mit Administratorrechten auf dem Gerät, auf dem Kaspersky Security Center Web Console installiert ist, die Installationsdatei der Kaspersky Security Center Web Console aus, die der auf Ihrem Gerät installierten Linux-Distribution entspricht.

     Der Installationsassistent wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

  2. Wählen Sie die Option **Aktualisieren** aus.

  3. Wählen Sie im Schritt **Änderungstyp** die Option **Verbindungseinstellungen ändern** aus.

  4. Fügen Sie im Schritt **Vertrauenswürdige Administrationsserver** den erforderlichen sekundären Administrationsserver hinzu.

  5. Klicken Sie im letzten Schritt auf **Ändern**, um die neuen Einstellungen zu übernehmen.

  6. Nach dem erfolgreichen Abschluss der Neukonfigurierung der Anwendung klicken Sie auf die Schaltfläche **Fertigstellen**.

- Verwenden Sie die Kaspersky Security Center Web Console, um eine direkte Verbindung mit dem sekundären Administrationsserver herzustellen auf dem der virtuelle Server erstellt wurde. Anschließend können Sie in Kaspersky Security Center Web Console zum virtuellen Administrationsserver wechseln.

Virtuelle Administrationsserver verwalten

Dieser Abschnitt beschreibt die folgenden Vorgänge für die Verwaltung von virtuellen Administrationsservern:

- Virtuelle Administrationsserver erstellen
- Virtuelle Administrationsserver aktivieren und deaktivieren
- Virtuellen Administrationsservern einen Administrator zuweisen
- Den Administrationsserver für Client-Geräte wechseln
- Virtuelle Administrationsserver löschen

Einen virtuellen Administrationsserver erstellen

Sie können virtuelle Administrationsserver erstellen und sie zu Administrationsgruppen hinzufügen.

Wenn Sie einen virtuellen Administrationsserver erstellen, erbt dieser die Benutzerliste und alle Benutzerrechte des primären Administrationsservers. Wenn ein Benutzer Zugriffsrechte auf den primären Server besitzt, hat dieser Benutzer auch Zugriffsrechte auf den virtuellen Server. Nach der Erstellung konfigurieren Sie die Zugriffsrechte auf die Server unabhängig.

Um einen virtuellen Administrationsserver zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.
2. Gehen Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.
3. Wählen Sie die Administrationsgruppe aus, zu der Sie den virtuellen Administrationsserver hinzufügen möchten. Der virtuelle Administrationsserver wird die Geräte dieser ausgewählten Gruppe (einschließlich der Untergruppen) verwalten.
4. Klicken Sie in der Menüleiste auf **Neuer virtueller Administrationsserver**.
5. Legen Sie auf der nächsten Seite die Eigenschaften des neuen virtuellen Administrationsservers fest:
   - **Name des virtuellen Administrationsservers**.
   - **Verbindungsadresse des Administrationsservers**

     Sie können den Namen oder die IP-Adresse Ihres Administrationsservers angeben.
6. Wählen Sie aus der Benutzerliste den Administrator des virtuellen Administrationsservers aus. Bei Bedarf können Sie vor der Zuweisung der Administratorrolle eines der vorhandenen Benutzerkonten bearbeiten oder ein neues Benutzerkonto erstellen.

   Bei Bedarf können Sie mithilfe des Tools "kladduser" ein neues Benutzerkonto anlegen, das als Administrator des virtuellen Administrationsservers fungiert. Verwenden Sie dazu den folgenden Befehl:

   `kladduser -n <Benutzername> -p <Kennwort> -vs <Name_des_virtuellen_Servers>`

   wobei `Name_des_virtuellen_Servers` für den Namen des virtuellen Administrationsservers steht.
7. Klicken Sie auf die Schaltfläche **Speichern**.

Der neue virtuelle Administrationsserver wird erstellt, zur Administrationsgruppe hinzugefügt und auf der Registerkarte **Administrationsserver** angezeigt.

Wenn Sie in der Kaspersky Security Center Web Console mit Ihrem primären Administrationsserver verbunden sind und keine Verbindung zu einem virtuellen Administrationsserver, der von einem sekundären Administrationsserver verwaltet wird, herstellen können, haben Sie folgende Möglichkeiten:

- **Ändern Sie die vorhandene Installation von Kaspersky Security Center Web Console, um den sekundären Server zur Liste der vertrauenswürdigen Administrationsserver hinzuzufügen.** Anschließend können Sie sich in Kaspersky Security Center Web Console mit dem virtuellen Administrationsserver verbinden.

  1. Führen Sie unter einem Konto mit Administratorrechten auf dem Gerät, auf dem Kaspersky Security Center Web Console installiert ist, die Installationsdatei der Kaspersky Security Center Web Console aus, die der auf Ihrem Gerät installierten Linux-Distribution entspricht.

     Der Installationsassistent wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.
  2. Wählen Sie die Option **Aktualisieren** aus.
  3. Wählen Sie im Schritt **Änderungstyp** die Option **Verbindungseinstellungen ändern** aus.

4. Fügen Sie im Schritt **Vertrauenswürdige Administrationsserver** den erforderlichen sekundären Administrationsserver hinzu.

5. Klicken Sie im letzten Schritt auf **Ändern**, um die neuen Einstellungen zu übernehmen.

6. Nach dem erfolgreichen Abschluss der Neukonfigurierung der Anwendung klicken Sie auf die Schaltfläche **Fertigstellen**.

- Verwenden Sie die Kaspersky Security Center Web Console, um eine direkte Verbindung mit dem sekundären Administrationsserver herzustellen auf dem der virtuelle Server erstellt wurde. Anschließend können Sie in Kaspersky Security Center Web Console zum virtuellen Administrationsserver wechseln.

Einen virtuellen Administrationsserver aktivieren und deaktivieren

Wenn Sie einen neuen virtuellen Administrationsserver erstellen, ist dieser standardmäßig aktiviert. Sie können ihn jederzeit aktivieren oder deaktivieren. Das Aktivieren oder Deaktivieren eines virtuellen Administrationsservers kommt dem Ein- und Ausschalten eines physischen Administrationsservers gleich.

Um einen virtuellen Administrationsserver zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

2. Wechseln Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.

3. Wählen Sie den virtuellen Administrationsserver aus, den Sie aktivieren oder deaktivieren möchten.

4. Klicken Sie auf der Menüleiste auf die Schaltfläche **Virtuellen Administrationsserver aktivieren / deaktivieren**.

Der Status des virtuellen Administrationsservers ändert sich abhängig vom vorherigen Status in "Aktiviert" oder "Deaktiviert". Der aktualisierte Status wird neben dem Namen des Administrationsservers angezeigt.

Einem virtuellen Administrationsserver einen Administrator zuweisen

Wenn Sie in Ihrem Unternehmen virtuelle Administrationsserver verwenden, möchten Sie möglicherweise jedem virtuellen Administrationsserver einen eigenen Administrator zuweisen. Dies kann beispielsweise nützlich sein, wenn Sie virtuelle Administrationsserver erstellen, um separate Büros oder Abteilungen Ihrer Organisation zu verwalten, oder wenn Sie ein MSP-Anbieter sind und Sie Ihre Mandanten über virtuelle Administrationsserver verwalten möchten.

Wenn Sie einen virtuellen Administrationsserver erstellen, erbt dieser die Benutzerliste und alle Benutzerrechte des primären Administrationsservers. Wenn ein Benutzer Zugriffsrechte auf den primären Server besitzt, hat dieser Benutzer auch Zugriffsrechte auf den virtuellen Server. Nach der Erstellung konfigurieren Sie die Zugriffsrechte auf die Server unabhängig. Wenn Sie einen Administrator für genau einen virtuellen Administrationsserver zuweisen möchten, stellen Sie sicher, dass der Administrator keine Zugriffsrechte auf dem primären Administrationsserver hat.

Sie weisen einem virtuellen Administrationsserver einen Administrator zu, indem Sie dem Administrator die Zugriffsrechte auf den virtuellen Administrationsserver gewähren. Sie können die erforderlichen Zugriffsrechte auf eine der folgenden Arten erteilen:

- Die Zugriffsrechte des Administrators manuell konfigurieren
- Dem Administrator eine oder mehrere Benutzerrollen zuweisen

Um sich an der Kaspersky Security Center Web Console anzumelden, gibt ein Administrator eines virtuellen Administrationsservers den Namen, den Benutzernamen und das Passwort an. Kaspersky Security Center Web Console authentifiziert den Administrator und öffnet den virtuellen Administrationsserver, für den der Administrator die Zugriffsrechte besitzt. Der Administrator kann nicht zwischen Administrationsservern wechseln.

Erforderliche Vorrausetzungen

Stellen Sie vor dem Beginn sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der virtuelle Administrationsserver wurde erstellt.
- Auf dem primären Administrationsserver haben Sie für den Administrator, den Sie dem virtuellen Administrationsserver zuweisen möchten ein Konto erstellt.
- Sie besitzen die Berechtigung **Objekt-ACLs ändern** in dem Funktionsbereich **Allgemeine Funktionen** → **Benutzerberechtigungen**.

Manuelles Konfigurieren der Zugriffsrechte

So weisen Sie einem virtuellen Administrationsserver einen Administrator zu:

1. Wechseln Sie zum erforderlichen virtuellen Administrationsserver:
   a. Wählen Sie im Hauptmenü einen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**), und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.
   b. Klicken Sie im neuen Navigationsbereich auf den Namen des erforderlichen virtuellen Administrationsservers.

      > Aus den Abschnitten **IP-Bereiche** und **Gelöschte Objekte** können Sie nicht zu einem virtuellen Administrationsserver wechseln.

      Im Hauptmenü ändert sich der Administrationsserver zu dem von Ihnen ausgewählten.
2. Wechseln Sie zu den Eigenschaften des Administrationsservers, indem Sie im Hauptmenü auf dessen Namen klicken.

   Alternativ können Sie im Navigationsbereich den Mauszeiger über den Namen des virtuellen Administrationsservers bewegen und anschließend auf das Einstellungssymbol (⚙) klicken.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
3. Klicken Sie auf der Registerkarte **Zugriffsrechte** auf die Schaltfläche **Hinzufügen**.

   Es öffnet sich eine zusammenfassende Liste der Benutzer des primären Administrationsservers und des aktuellen virtuellen Administrationsservers.

4. Wählen Sie aus der Benutzerliste das Konto des Administrators aus, das Sie dem virtuellen Administrationsserver zuweisen möchten, und klicken Sie anschließend auf die Schaltfläche **OK**.

   Die Anwendung fügt den ausgewählten Benutzer der Benutzerliste auf der Registerkarte **Zugriffsrechte** hinzu.

5. Aktivieren Sie das Kontrollkästchen neben dem hinzugefügten Konto und klicken Sie auf die Schaltfläche **Zugriffsrechte**.

6. Konfigurieren Sie die Rechte, die der Administrator auf dem virtuellen Administrationsserver bekommen soll.

   Um sich erfolgreich anzumelden, muss der Administrator mindestens über die folgenden Berechtigungen verfügen:

   - Berechtigung **Lesen** im Funktionsbereich **Allgemeine Funktionen → Basisfunktionen**
   - Berechtigung **Lesen** im Funktionsbereich **Allgemeine Funktionen → Virtuelle Administrationsserver**

Die Anwendung speichert die geänderten Benutzerrechte im Administratorkonto.

So weisen Sie mehreren virtuellen Administrationsservern einen Administrator zu:

1. Klicken Sie im Hauptmenü auf den Namen des primären Administrationsservers.

2. Wechseln Sie auf der angezeigten Seite zur Registerkarte **Zugriffsrechte** und klicken Sie anschließend auf **Zuweisen**.

   Aktivieren Sie im sich öffnenden Fenster „**Benutzer oder Gruppen hinzufügen**“ das Kontrollkästchen neben dem Benutzer, den Sie als Administrator zuweisen möchten.

3. Sie können zur Registerkarte „**Gruppen**“ wechseln, um die Benutzergruppen auszuwählen.

4. Klicken Sie auf die Schaltfläche **Weiter**.

5. Wählen Sie die Server aus, denen Sie einen Administrator zuweisen möchten, und klicken Sie anschließend auf **Weiter**.

   Bei Auswahl von zwei oder mehr virtuellen Servern wird automatisch der Zugriff auf deren primären Administrationsserver gewährt. In diesem Fall kann diese Auswahl nicht aufgehoben werden, ohne die Auswahl der virtuellen Server zu löschen.

6. Wählen Sie bei Bedarf die Administratorrollen aus, die Sie für den Benutzer festlegen möchten.

   Wenn Sie für den Benutzer benutzerdefinierte Rollen für den aktuellen Administrationsserver festlegen möchten, wechseln Sie zu den Eigenschaften des erforderlichen Administrationsservers, klicken Sie auf **Rollen festlegen** und wählen Sie anschließend die benutzerdefinierten Rollen aus.

7. Klicken Sie auf **Fertigstellen**, um die Änderungen zu übernehmen.

Der Administrator mit den ausgewählten Rollen ist jetzt mehreren virtuellen Administrationsservern zugewiesen.

So entziehen Sie die Zugriffsrechte des Administrators:

1. Wechseln Sie zum erforderlichen virtuellen Administrationsserver.

2. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

3. Wechseln Sie auf der nächsten Seite auf die Registerkarte „**Zugriffsrechte**“.

4. Aktivieren Sie das Kontrollkästchen neben dem Benutzer, dem Sie die Zugriffsrechte entziehen möchten.

5. Klicken Sie auf „**Widerrufen**“ und bestätigen Sie Ihre Aktion.

Die Zugriffsrechte des ausgewählten Benutzers werden entzogen.

Konfigurieren der Zugriffsrechte durch Zuweisen von Benutzerrollen

Alternativ können Sie einem Administrator des virtuellen Administrationsservers die Zugriffsrechte über Benutzerrollen zuweisen. Dies kann beispielsweise nützlich sein, wenn Sie mehrere Administratoren auf demselben virtuellen Administrationsserver zuweisen möchten. In diesem Fall können Sie den Konten der Administratoren die gleiche oder mehrere Benutzerrollen zuweisen, anstatt für mehrere Administratoren die gleichen Benutzerrechte zu konfigurieren.

So weisen Sie einem virtuellen Administrationsserver einen Administrator durch Zuweisung von Benutzerrollen zu:

1. Erstellen Sie eine neue Benutzerrolle auf dem primären Administrationsserver und legen Sie anschließend alle erforderlichen Zugriffsrechte fest, die ein Administrator auf dem virtuellen Administrationsserver bekommen soll. Sie können mehrere Rollen anlegen, wenn Sie beispielsweise den Zugriff auf verschiedene Funktionsbereiche trennen möchten.

2. Wechseln Sie zum erforderlichen virtuellen Administrationsserver:

   a. Wählen Sie im Hauptmenü einen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**), und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

   b. Klicken Sie im neuen Navigationsbereich auf den Namen des erforderlichen virtuellen Administrationsservers.

   > Aus den Abschnitten **IP-Bereiche** und **Gelöschte Objekte** können Sie nicht zu einem virtuellen Administrationsserver wechseln.

   Im Hauptmenü ändert sich der Administrationsserver zu dem von Ihnen ausgewählten.

3. Weisen Sie die neue Rolle oder mehrere Rollen dem Administratorkonto zu.

Die Anwendung weist dem Administratorkonto die neue Rolle zu.

Konfigurieren der Zugriffsrechte auf Objektebene

Neben der Zuweisung von Zugriffsrechten auf Ebene von Funktionsbereichen können Sie auch den Zugriff auf bestimmte Objekte konfigurieren, die sich auf dem virtuellen Administrationsserver befinden, beispielsweise einer bestimmten Administrationsgruppe oder Aufgabe. Wechseln Sie dazu auf den virtuellen Administrationsserver und konfigurieren Sie anschließend die Zugriffsrechte in den Eigenschaften des Objekts.

Administrationsserver für Client-Geräte wechseln

Mit der Aufgabe *Administrationsserver wechseln* wechseln können Sie den Administrationsserver, der die Client-Geräte verwaltet, durch einen anderen Administrationsserver ersetzen. Nach Abschluss der Aufgabe werden die Client-Geräte unter die Verwaltung des Administrationsservers gestellt, denn Sie angegeben haben.

Sie können die Aufgabe *Administrationsserver wechseln* nicht für Client-Geräte verwenden, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind. Für solche Geräte müssen Sie entweder den Administrationsagenten neu konfigurieren oder den Administrationsagenten neu installieren und das Verbindungs-Gateway angeben.

So ändern Sie einen Administrationsserver, der die Client-Geräte verwaltet:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.
3. Geben Sie im Schritt **Einstellungen der neue Aufgabe** des Assistenten die folgenden Einstellungen an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Security Center** aus.

   b. Wählen Sie im Feld **Aufgabentyp** die Option **Administrationsserver wechseln** aus.

   c. Geben Sie im Feld **Aufgabenname** den Namen für die Aufgabe an, die Sie erstellen.

   Der Aufgabenname darf höchstens 100 Zeichen lang sein und darf keine Sonderzeichen ("*<>?\:|) enthalten.

   d. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

   - **Geräteadressen manuell angeben oder aus Liste importieren**

     Sie können DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die Aufgabe zugewiesen werden soll.

     Diese Option können Sie beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

4. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** des Assistenten eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Auswahl an Geräten an.

5. Bestätigen Sie in diesem Schritt des Assistenten, dass Sie den Bedingungen für das Wechseln des Administrationsservers für Client-Geräte zustimmen.

6. Wählen Sie in diesem Schritt des Assistenten den Administrationsserver aus, den Sie für die Verwaltung der ausgewählten Geräte verwenden möchten:

   - **Zu einem anderen primären Administrationsserver wechseln**

     Um Client-Geräte auf einen anderen primären Administrationsserver zu verschieben, geben Sie die folgenden Verbindungseinstellungen für den Administrationsserver an:

     1. Geben Sie im Feld **Adresse des Administrationsservers** die Adresse des neuen primären Administrationsservers an.

     2. Geben Sie im Feld **Port** die Portnummer für die Verbindung zum Administrationsserver an.

        Standardmäßig wird die Portnummer 14000 verwendet.

     3. Geben Sie im Feld **SSL-Port** die Nummer des SSL-Ports auf dem primären Administrationsserver an

        Standardmäßig wird die Portnummer 13000 verwendet.

     4. Aktivieren Sie bei Bedarf die Option **Proxyserver verwenden**.

        Wenn diese Option deaktiviert ist, wird die direkte Verbindung genutzt, um das Gerät mit dem Administrationsserver zu verbinden.

        Wenn diese Option aktiviert ist, geben Sie die Parameter des Proxyservers an:

        - **Proxyserver-Adresse**

        - **Proxyserver-Port**

        Falls Ihr Proxyserver eine Authentifizierung erfordert, geben Sie in den Feldern **Benutzername** und **Kennwort** die Anmeldeinformationen des Kontos ein, unter dem die Verbindung mit dem Proxyserver hergestellt wird. Es wird empfohlen, dass Sie die Anmeldeinformationen für ein Konto angeben, das lediglich über die Mindestberechtigungen verfügt, die für die Proxyserver-Authentifizierung erforderlich sind.

     5. Laden Sie bei Bedarf ein neues Zertifikat für den Administrationsserver hoch.

   - **Auf diesem primären Server zu einem anderen virtuellen Server wechseln**

     Wählen Sie diese Option aus, um die Client-Geräte zu einem virtuellen Administrationsserver auf dem aktuellen primären Administrationsserver verschieben. Wählen Sie dazu in der Dropdown-Liste **Name des virtuellen Administrationsservers** den gewünschten virtuellen Administrationsserver aus.

7. Geben Sie im Schritt **Benutzerkonto für die Ausführung der Aufgabe auswählen** des Assistenten die Kontoeinstellungen an:

   - **Standardbenutzerkonto**

     Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

     Diese Variante ist standardmäßig ausgewählt.

   - **Benutzerkonto festlegen**

     Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

     - **Benutzerkonto**

       Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

     - **Kennwort**

       Kennwort des Benutzerkontos, unter dem die Aufgabe ausgeführt wird.

8. Wenn Sie die standardmäßigen Aufgabeneinstellungen ändern möchten, aktivieren Sie auf in dem Schritt **Erstellung der Aufgabe abschließen** des Assistenten die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**.

   Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

10. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

11. Wenn Sie die standardmäßigen Aufgabeneinstellungen ändern möchten, geben Sie im Fenster mit den Aufgabeneigenschaften die allgemeinen Aufgabeneinstellungen entsprechend Ihren Bedürfnissen an.

12. Klicken Sie auf die Schaltfläche **Speichern**.

    Die Aufgabe wird erstellt und konfiguriert.

13. Starten Sie die erstellte Aufgabe.

Nach Abschluss der Aufgabe werden die Client-Geräte, für welche die Aufgabe erstellt wurde, auf den Administrationsserver umgestellt, der in den Einstellungen der Aufgabe angegeben wurde.

Einen virtuellen Administrationsserver löschen

Wenn Sie einen virtuellen Administrationsserver löschen, werden auch alle Objekte gelöscht, die auf dem virtuellen Administrationsserver erstellt wurden, inklusive Richtlinien und Aufgaben. Die verwalteten Geräte aus den Administrationsgruppen, die von dem virtuellen Administrationsserver verwaltet wurden, werden aus den Administrationsgruppen entfernt. Um die Geräte erneut in die Verwaltung durch Kaspersky Security Center Linux aufzunehmen, müssen Sie eine Netzwerkabfrage durchführen und die gefundenen Geräte aus der Gruppe "Nicht zugeordnete Geräte" in die Administrationsgruppe verschieben.

So löschen Sie einen virtuellen Administrationsserver:

1. Wechseln Sie zum primären physischen Administrationsserver, zu dem der zu löschende virtuelle Administrationsserver gehört:

   a. Wählen Sie im Hauptmenü einen beliebigen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**), und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

   b. Klicken Sie im neuen Navigationsbereich auf den Namen des primären physischen Administrationsservers.

   Im Hauptmenü ändert sich der Administrationsserver zu dem von Ihnen ausgewählten.

2. Wechseln Sie auf eine der folgenden Arten zu den Eigenschaften des primären physischen Administrationsservers:

   - Bewegen Sie im Navigationsbereich den Mauszeiger über den Namen des erforderlichen Administrationsservers und klicken Sie anschließend auf das Einstellungssymbol (⚙).

   - Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

3. Wechseln Sie im neuen Eigenschaftsfenster zur Registerkarte **Administrationsserver**.

4. Wählen Sie den virtuellen Administrationsserver aus, den Sie löschen möchten.

5. Klicken Sie in der Menüleiste auf **Löschen**.

Der virtuelle Administrationsserver wurde gelöscht.

Protokollierung der Verbindungsereignisse des Administrationsservers konfigurieren

Der Verlauf der Verbindungen und Versuche, während des Betriebs eine Verbindung mit dem Administrationsserver herzustellen, können in einer Protokolldatei gespeichert werden. Mit den Informationen in der Datei können Sie nicht nur Verbindungen innerhalb Ihrer Netzwerkinfrastruktur verfolgen, sondern auch nicht autorisierte Versuche, auf den Server zuzugreifen.

So protokollieren Sie die Ereignisse der Verbindung zum Administrationsserver:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verbindungsports** aus.

3. Aktivieren Sie die Option **Verbindungsereignisse des Administrationsservers protokollieren**.

Alle weiteren Ereignisse eingehender Verbindungen zum Administrationsserver, Authentifizierungsergebnisse und SSL-Fehler werden in der Datei /var/opt/kaspersky/klnagent_srv/logs/SC.syslog.

Maximalen Anzahl an Ereignissen in der Ereignis-Datenverwaltung festlegen

Im Eigenschaftenfenster des Administrationsservers können Sie im Abschnitt **Ereignis-Datenverwaltung** die Einstellungen für das Speichern der Ereignisse in der Administrationsserver-Datenbank anpassen: Anzahl der Einträge über Ereignisse und Speicherdauer der Einträge beschränken. Wenn Sie die maximale Anzahl der Ereignisse angeben, berechnet die Anwendung einen ungefähren Wert des für die angegebene Zahl benötigten Speicherplatzes. Sie können diese ungefähre Berechnung verwenden, um zu überprüfen, ob Sie ausreichen freien Platz auf dem Laufwerk haben, um einen Überlauf der Datenbank zu vermeiden. Standardmäßig umfasst die Administrationsserver-Datenbank 400.000 Ereignisse. Die empfohlene Maximalgröße der Datenbank liegt bei 45 Millionen Ereignissen.

Die Anwendung überprüft die Datenbank alle 10 Minuten. Wenn die Anzahl der Ereignisse den festgelegten Höchstwert plus 10.000 erreicht, löscht die Anwendung die ältesten Ereignisse, sodass nur noch die festgelegte Höchstanzahl von Ereignissen übrig bleibt.

Wenn der Administrationsserver alte Ereignisse löscht, kann er keine neuen Ereignisse in der Datenbank speichern. Während diese Vorgangs werden Informationen über abgelehnte Ereignisse in das Betriebssystem-Protokoll geschrieben. Die neuen Ereignisse werden in die Warteschlange verschoben und dann in der Datenbank gespeichert, nachdem der Löschvorgang abgeschlossen wurde. Die Warteschlange für Ereignisse ist standardmäßig auf 20.000 Ereignisse beschränkt. Sie können die Beschränkung der Warteschlange anpassen, indem Sie den Wert des Flags KLEVP_MAX_POSTPONED_CNT ändern.

Um die Anzahl der Ereignisse, die in der Ereignis-Datenverwaltung des Administrationsservers gespeichert werden können, zu begrenzen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Ereignis-Datenverwaltung** aus. Geben Sie die maximale Anzahl von Ereignissen an, die in der Datenbank gespeichert sind.

3. Klicken Sie auf die Schaltfläche **Speichern**.

Zusätzlich können Sie Folgendes tun:

- Die Einstellungen einer beliebigen Aufgabe ändern, um entweder Ereignisse im Zusammenhang mit dem Aufgabenfortschritt oder nur die Ergebnisse der Aufgabenausführung zu speichern.

- Die Speicherdauer verkürzen oder deaktivieren für Ereignisse des Administrationsservers, des Administrationsagenten und der Kaspersky-Anwendungen, die auf den verwalteten Geräten installiert sind.

Auf diese Weise reduzieren Sie die Anzahl der Ereignisse in der Datenbank, erhöhen die Ausführungsgeschwindigkeit der Szenarien, die mit der Analyse der Ereignistabelle in der Datenbank verbunden sind, und reduzieren das Risiko der Verdrängung von kritischen Ereignissen durch eine große Anzahl an Ereignissen.

Administrationsserver auf anderes Gerät übertragen

Wenn Sie den Administrationsserver auf einem neuen Gerät verwenden müssen, können Sie ihn auf eine der folgenden Arten verschieben:

- Verschieben Sie den Administrationsserver und den Datenbankserver auf ein neues Gerät (der Datenbankserver kann auf dem neuen Gerät zusammen mit dem Administrationsserver oder auf einem anderen Gerät installiert werden).
- Belassen Sie den Datenbankserver auf dem bisherigen Gerät und verschieben Sie nur den Administrationsserver auf ein neues Gerät.

So verschieben Sie Administrationsserver und den Datenbankserver auf ein neues Gerät:

1. Erstellen Sie auf dem bisherigen Gerät ein Backup der Daten des Administrationsservers.

   Dazu können Sie entweder die Aufgabe zum Anlegen eines Daten-Backups in der Kaspersky Security Center Web Console verwenden oder das Tool klbackup ausführen.

2. Trennen Sie den Administrationsserver auf dem vorherigen Gerät vom Netzwerk.

3. Wählen Sie ein neues Gerät aus, auf dem der Administrationsserver installiert werden soll. Stellen Sie sicher, dass die Hardware und Software des ausgewählten Gerätes den Anforderungen für den Administrationsserver, für Kaspersky Security Center Web Console und für den Administrationsagenten entsprechen. Überprüfen Sie außerdem, ob die auf dem Administrationsserver verwendeten Ports verfügbar sind.

4. Weisen Sie dem neuen Gerät dieselbe Adresse zu.

   Dem neuen Administrationsserver können der NetBIOS-Name, der FQDN und die statische IP-Adresse zugewiesen werden. Dies hängt davon ab, welche Adresse für den Administrationsagenten im Installationspaket des Administrationsagenten angegeben wurde, als die Administrationsagenten verteilt wurden. Alternativ können Sie die Verbindungsadresse verwenden, die den Administrationsserver bestimmt, mit dem der Administrationsagent eine Verbindung herstellt (diese Adresse kann auf verwalteten Geräten mithilfe des Tools klnagchk ermittelt werden).

5. Installieren Sie das Datenbankverwaltungssystem (DBMS) bei Bedarf auf einem anderen Gerät, das vom Administrationsserver verwenden wird.

   Die Datenbank kann entweder zusammen mit dem Administrationsserver auf dem neuen Gerät oder auf einem anderen Gerät installiert werden. Stellen Sie sicher, dass dieses Gerät die Hard- und Softwarevoraussetzungen erfüllt. Berücksichtigen Sie bei der Auswahl eines DBMS die Anzahl der vom Administrationsserver verwalteten Geräte.

6. Installieren Sie den Administrationsserver auf dem neuen Gerät.

   Hinweis: Wenn Sie den Datenbankserver auf ein anderes Gerät verschieben, müssen Sie die lokale Adresse als IP-Adresse des Gerätes angeben, auf dem die Datenbank installiert ist (Element "h" in der Anweisung zur Installation von Kaspersky Security Center Linux). Wenn Sie den Datenbankserver auf dem bisherigen Gerät belassen müssen, geben Sie die IP-Adresse des bisherigen Geräts im Element "h" der Anweisung Kaspersky Security Center Linux installieren an.

7. Stellen Sie nach Abschluss der Installation die Administrationsserver-Daten auf dem neuen Gerät mithilfe des Tools "klbackup" wieder her.

8. Öffnen Sie Kaspersky Security Center Web Console und stellen Sie eine Verbindung zum Administrationsserver her.

9. Überprüfen Sie, ob alle verwalteten Geräte mit dem Administrationsserver verbunden sind.

10. Deinstallieren Sie den Administrationsserver und den Datenbankserver vom bisherigen Gerät.

DBMS-Anmeldedaten ändern

In einigen Fällen müssen Sie möglicherweise die DBMS-Anmeldedaten ändern, beispielsweise um aus Sicherheitsgründen eine Rotation der Anmeldedaten auszuführen.

Ändern der Anmeldeinformationen für die Datenbank des Administrationsservers

So ändern Sie die Anmeldeinformationen für die Datenbank des Administrationsservers in einer Linux-Umgebung mittels des Tools "klsrvconfig":

1. Beenden Sie den Administrationsserver. Führen Sie die folgenden Befehle aus:

   ```
   systemctl stop kladminserver_srv.service
   systemctl stop klnagent_srv.service
   systemctl stop klactprx_srv.service
   systemctl stop klwebsrv_srv.service
   ```

2. Starten Sie das Tool "klsrvconfig".

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

3. Geben Sie einen neuen Kontonamen an. Sie sollten die Anmeldedaten eines Benutzerkontos angeben, das im DBMS vorhanden ist.

4. Geben Sie ein neues Kennwort ein.

5. Geben Sie das neue Kennwort erneut zur Bestätigung ein.

6. Starten Sie den Administrationsserver. Führen Sie die folgenden Befehle aus:

   ```
   systemctl start kladminserver_srv.service
   systemctl start klnagent_srv.service
   systemctl start klactprx_srv.service
   systemctl start klwebsrv_srv.service
   ```

Die Anmeldeinformationen für die Datenbank des Administrationsservers wurden geändert.

Ändern der Anmeldeinformationen für die IAM-Datenbank

So ändern Sie die Anmeldeinformationen für die IAM-Datenbank in einer Linux-Umgebung mittels Änderung der Konfigurationsdatei:

1. Beenden Sie den Administrationsserver. Führen Sie die folgenden Befehle aus:

   ```
   systemctl stop kladminserver_srv.service
   systemctl stop klnagent_srv.service
   ```

```
systemctl stop klactprx_srv.service
systemctl stop klwebsrv_srv.service
```

2. Öffnen Sie die IAM-Konfigurationsdatei unter /var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml
3. Geben Sie im Abschnitt `dbms_iam` die neuen Anmeldeinformationen des Kontos in den Feldern für Nutzername und Kennwort ein. Sie sollten die Anmeldedaten eines Benutzerkontos angeben, das im DBMS vorhanden ist.
4. Starten Sie den Administrationsserver. Führen Sie die folgenden Befehle aus:

```
systemctl start kladminserver_srv.service
systemctl start klnagent_srv.service
systemctl start klactprx_srv.service
systemctl start klwebsrv_srv.service
```

Die Anmeldeinformationen für die IAM-Datenbank wurden geändert.

Backup-Kopie der Daten des Administrationsservers anlegen und wiederherstellen

Die Datensicherung ermöglicht es Ihnen, den Administrationsserver ohne Datenverlust von einem Gerät auf ein anderes zu übertragen. Durch das Backup können Sie die Daten wiederherstellen, wenn Sie die Administrationsserver-Datenbank auf ein anderes Gerät verschieben oder ein Upgrade auf eine neuere Version von Kaspersky Security Center durchführen. Sie können ein Daten-Backup auch dazu verwenden, um die Daten eines Administrationsservers für Kaspersky Security Center Windows unter die Verwaltung von Kaspersky Security Center Linux zu verschieben (das Verschieben der Daten von Kaspersky Security Center Linux nach Kaspersky Security Center Windows wird nicht unterstützt).

Die installierten Verwaltungs-Plug-ins werden nicht mittels Backup gesichert. Nachdem Sie die Daten des Administrationsservers aus einer Sicherungskopie wiederhergestellt haben, müssen Sie Plug-ins für die verwalteten Anwendungen herunterladen und neu installieren.

Bevor Sie die Daten des Administrationsservers sichern, führen Sie die folgenden Aktionen durch:

- **Befolgen Sie die Anforderungen zum Erstellen einer Sicherung auf Administration Server 16 oder früher und zum Wiederherstellen dieser Sicherung in Version 16.1 oder später.**

  - Wenn Sie eine Datensicherung auf Administration Server 16 oder früher erstellen und diese auf Administration Server 16.1 oder später wiederherstellen, wird die Zwei-Faktor-Authentifizierung aktiviert. Weitere Informationen finden Sie unter Über die Zwei-Faktor-Authentifizierung für ein Konto.

    Um sicherzustellen, dass Benutzer Bei der Webkonsole anmelden mit ihren bestehenden Konten unter Verwendung konfigurierter geheimer Schlüssel für die Zwei-Faktor-Authentifizierung, und dass OpenAPI-Automatisierungsskripte Um nach der Wiederherstellung weiterarbeiten zu können, müssen Sie die folgenden Schritte ausführen:

    - Zwei-Faktor-Authentifizierung für alle Benutzer aktivieren
    - Administratoren müssen die Zwei-Faktor-Authentifizierung für ihre eigenen Konten konfigurieren

- Die erforderlichen Konten von der Zwei-Faktor-Authentifizierung ausschließen

  Fügen Sie bei Bedarf Integrationskonten, die zum Ausführen von Skripten über OpenAPI verwendet werden, zur Ausschlussliste hinzu.

Wenn es nicht möglich ist, die Zwei-Faktor-Authentifizierung vor dem Erstellen des Backups zu konfigurieren, werden Benutzerkonten zur Allow-Liste für die Zwei-Faktor-Authentifizierung hinzugefügt und können die Zwei-Faktor-Authentifizierung bei der Anmeldung an der Web Console konfiguriert werden. Ausführlichere Bedingungen für das Hinzufügen eines Kontos zur Allow-Liste sind im Thema beschrieben Benutzern die Konfiguration der Zwei-Faktor-Authentifizierung ermöglichen.

- Überprüfen Sie, ob ein virtueller Administrationsserver zur Administrationsgruppe hinzugefügt wurde. Sollte ein virtueller Administrationsserver hinzugefügt worden sein, stellen Sie vor dem Backup sicher, dass dem virtuellen Administrationsserver ein Administrator zugewiesen ist. Nach dem Backup können Sie für den virtuellen Administrationsserver keine Administratorrechte mehr vergeben. Beachten Sie, dass im Sie im Falle des Verlusts der Anmeldeinformationen des Administrators nicht mehr in der Lage sind, dem virtuellen Administrationsserver einen neuen Administrator zuzuweisen.

- Wenn Sie einen Kaspersky Security Center-Failover-Cluster sichern oder wiederherstellen möchten, müssen Sie den gesamten Cluster zur Wartung anhalten und anschließend neu starten, wenn die Sicherung oder Wiederherstellung abgeschlossen ist.

Sie können eine Backup-Kopie der Daten des Administrationsservers auf eine der folgenden Weisen erstellen:

- Erstellen und Ausführen einer Aufgabe zum Anlegen eines Daten-Backups über Kaspersky Security Center Web Console.

- Das Tool klbackup auf einem Gerät mit dem installierten Administrationsserver starten. Dieses Tool gehört zum Lieferumfang von Kaspersky Security Center. Es befindet sich nach der Installation des Administrationsservers im Stammverzeichnis des Zielordners, der bei der Installation der Anwendung angegeben wurde (gewöhnlich im Ordner /opt/kaspersky/ksc64/sbin/klbackup).

In der Backup-Kopie der Daten des Administrationsservers werden folgende Daten gespeichert:

- Administrationsserver-Datenbank (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse).

- Konfigurationsdaten über die Struktur der Administrationsgruppen und Client-Geräte.

- Speicherort der Programmpakete für die Remote-Installation.

- Zertifikat des Administrationsservers.

- Für Benutzerkonten konfigurierte geheime Schlüssel für die Zwei-Faktor-Authentifizierung.

- Liste der Benutzerkonten, die von der Zwei-Faktor-Authentifizierung ausgeschlossen sind.

Sie können ein Backup der Daten des Administrationsservers anlegen erstellen, indem Sie entweder eine Datensicherungsaufgabe erstellen und ausführen oder das Dienstprogramm klbackup verwenden. Die Wiederherstellung von Daten des Administrationsservers ist nur mit dem Dienstprogramm klbackup möglich. Sie müssen die Wiederherstellung auf einer funktionierenden Instanz des Administrationsservers durchführen, die gerade installiert wurde und die gleiche Version (oder höher) besitzt, für welche die Sicherung erstellt wurde. Verwenden Sie keine Tools von Drittanbietern für die Backup und Wiederherstellung, und entfernen Sie nach Möglichkeit die vorherige Installation von Kaspersky Security Center Linux nicht, bis die Konfiguration und die Datenübertragung vollständig abgeschlossen sind.

Sicherungsaufgabe für die Daten des Administrationsserver erstellen

Backup-Aufgaben gehören zu den Aufgaben des Administrationsservers und werden mit dem Schnellstartassistenten erstellt. Wenn die vom Schnellstartassistenten erstellte Aufgabe zum Anlegen eines Backups gelöscht wurde, können Sie diese manuell erstellen.

Die Aufgabe *Backup der Daten des Administrationsservers anlegen* kann nur einmal erstellt werden. Wenn die Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers für den Administrationsserver bereits erstellt wurde, wird sie im Fenster für die Auswahl des Aufgabentyps nicht angezeigt.

So erstellen Sie eine Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.
3. Wählen Sie in der Liste **Anwendung** die Option **Kaspersky Security Center 16.3** und in der Liste **Aufgabentyp** die Option **Backup der Daten des Administrationsservers anlegen** aus.
4. Geben Sie im entsprechenden Schritt die folgenden Informationen an:
   - Ordner zum Speichern der Backup-Kopien
   - Kennwort für das Backup (optional)
   - Maximale Anzahl zu speichernder Backup-Kopien
5. Wenn Sie im Schritt **Erstellung der Aufgabe abschließen** die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, können Sie die standardmäßigen Aufgabeneinstellungen ändern. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.
6. Klicken Sie auf die Schaltfläche **Fertigstellen**.

Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

Tool "klbackup" zum Sichern und Wiederherstellen von Daten verwenden

Sie können die Daten des Administrationsservers mittels des Tools klbackup, welches im Lieferumfang von Kaspersky Security Center enthalten ist, zum Zweck eines Backups und späterer Wiederherstellung kopieren.

Die Instanz des Administrationsservers, auf der die Wiederherstellung ausgeführt werden soll, muss ein DBMS desselben Typs verwenden. Die Version des Administrationsservers kann gleich (mit einem ähnlichen oder neueren Patch) oder neuer sein.

Wenn Sie in Kaspersky Security Center Linux 15 oder früher die Daten des Administrationsservers mittels einer früheren Version des MariaDB-DBMS gesichert haben, und die Daten anschließend auf einem Gerät mit einer aktuelleren Version von MariaDB wiederherstellen, kann es zu einem Fehler kommen. Weitere Informationen finden Sie unter Wiederherstellung der Administrationsserver-Daten aus einem Backup, das mit einer früheren Version von DBMS angelegt wurde.

Bei Verwendung des Tools "klbackup" werden die Flags des Administrationsagenten nicht wiederhergestellt. Sie müssen die Flags des Administrationsagenten manuell konfigurieren.

So erstellen Sie eine Backup-Kopie der Daten oder stellen die Daten des Administrationsservers im Silent-Modus wieder her:

Starten Sie aus der Befehlszeile des Geräts, auf dem der Administrationsserver installiert ist, das Tool klbackup mit der erforderlichen Auswahl an Schlüsseln.

Die Befehlszeilensyntax des Tools lautet:

```
klbackup -path <Backup-Pfad> [-linux_path <DBMS-Backup-Pfad>-node_cert <Zertifikat-Pfad>] [-logfile <Log-Datei> [-use_ts]|[-restore] [-password <Kennwort>] [-cert_only]
```

Wenn in der Befehlszeile des Tools klbackup kein Kennwort eingegeben wird, fragt das Tool das Kennwort interaktiv ab.

Beschreibung der Parameter:

- `-path <Backup-Pfad>` – Daten im Backup-Ordner speichern bzw. aus dem Backup-Ordner wiederherstellen (Pflichtparameter).
- `-linux_path <DBMS-Backup-Pfad>` – Lokaler Pfad zum Ordner mit den Backup-Daten des DBMS.

  Das Benutzerkonto der Server-Datenbank und das klbackup-Tool müssen über die Berechtigung zum Ändern der Daten im DBMS-Backup-Ordner verfügen.
- `-node_cert <Zertifikat-Pfad>` – Server-Zertifikatsdatei zum Konfigurieren inaktiver Failover-Cluster-Knoten nach der Wiederherstellung. Wenn kein Pfad festgelegt ist, wird er automatisch vom Server abgerufen.
- `-logfile <Log-Datei>` – Bericht über das Anlegen und Wiederherstellen eines Daten-Backups des Administrationsservers speichern.

  Das Benutzerkonto der Server-Datenbank und das klbackup-Tool müssen über die Berechtigung zum Ändern der Daten im Backup-Ordner verfügen.
- `-use_ts` – Kopiert beim Speichern die Informationen in einen Unterordner des Backup-Ordners, wobei der Name des Unterordners im Format `klbackup YYYY-MM-DD # HH-MM-SS` angegeben ist und die aktuelle UTC-Zeit enthält. Wenn der Schlüssel nicht eingegeben wurde, werden die Angaben im Stammverzeichnis des Backup-Ordners abgelegt.

  Wenn Sie versuchen, die Informationen in einem Ordner zu speichern, in dem bereits eine Backup-Kopie vorhanden ist, erscheint eine Fehlermeldung. Die Informationen werden nicht aktualisiert.

Mit dem Schlüssel `-use_ts` kann ein Datenarchiv des Administrationsservers angelegt werden. Wenn z. B. mit dem Schlüssel `-path` der Ordner `/tmp/KLBackups` vorgegeben wurde, werden im Ordner `klbackup 2022/6/19 # 11-30-18` Informationen über den Status des Administrationsservers mit Stand vom 19. Juni 2022 um 11 Uhr, 30 Minuten und 18 Sekunden abgelegt.

- `-restore` – Daten des Administrationsservers wiederherstellen. Die Wiederherstellung der Daten erfolgt anhand der Informationen, die sich im Backup-Ordner befinden. Wenn kein Schlüssel vorhanden ist, werden die Daten im Backup-Ordner gesichert.

- `-password <Kennwort>` – Kennwort zum Schutz der vertraulichen Daten.

  Ein vergessenes Kennwort kann nicht wiederhergestellt werden. Es gibt keine Kennwortanforderungen. Die Kennwortlänge ist unbegrenzt und eine Länge von Null (kein Kennwort) ist ebenfalls möglich.

  Beim Wiederherstellen der Daten muss dasselbe Kennwort eingegeben werden wie beim Verschieben ins Backup. Wenn der Pfad zum freigegebenen Ordner nach dem Verschieben ins Backup verändert wird, muss nach der Wiederherstellung der Daten die Funktion jener Aufgaben überprüft werden, bei denen die wiederhergestellten Daten verwendet werden (Wiederherstellungsaufgaben, Remote-Installation). Erforderlichenfalls müssen die Einstellungen dieser Aufgaben geändert werden. Während der Wiederherstellung von Daten aus dem Backup darf der freigegebene Ordner des Administrationsservers von niemandem verwendet werden. Das Benutzerkonto, unter dem das Tool klbackup gestartet wird, muss über vollen Zugriff auf den freigegebenen Ordner verfügen. Um die Daten des Administrationsservers aus dem Backup wiederherzustellen, wird es empfohlen, das Tool auf einem neu installierten Administrationsserver auszuführen.

- `-cert_only` – Nur das Zertifikat und den privaten Schlüssel des Administrationsservers speichern oder wiederherstellen.

  Dieses Flag kann nützlich sein, wenn Sie eine Migration von einem Administrationsserver für Kaspersky Security Center Windows auf einen Administrationsserver für Kaspersky Security Center Linux durchführen. Darüber hinaus erlaubt es Ihnen die Migration verwalteter Geräte zwischen Administrationsservern für Kaspersky Security Center Linux und zwischen Administrationsservern für Kaspersky Security Center Windows.

Sie können ein Daten-Backup verwenden, um die Daten des Administrationsservers für Kaspersky Security Center Windows unter die Verwaltung von Kaspersky Security Center Linux zu verschieben.
Wenn Sie MySQL oder MariaDB als DBMS für Kaspersky Security Center Windows und für Kaspersky Security Center Linux verwenden, muss der Parameter `lower_case_table_names` für das aktuelle und das neue DBMS übereinstimmen.
Überprüfen Sie daher den Parameter `lower_case_table_names`, bevor Sie ein Daten-Backup anlegen. Wenn Sie anschließend MySQL oder MariaDB für Kaspersky Security Center Linux installieren, müssen Sie dem Parameter `lower_case_table_names` den gleichen Wert zuweisen, wie er für den Parameter unter Windows angegeben war.

Falls während der Wiederherstellung das Common Certificate des Administrationsservers durch ein anderes Zertifikat aus einer Sicherung ersetzt wird, führen Sie die folgenden Schritte durch, um einen ordnungsgemäßen Betrieb zu gewährleisten:
1. Installieren Sie die Web Console erneut, um den folgenden Fehler zu vermeiden:
Der Administrationsserver verwendet ein nicht vertrauenswürdiges Zertifikat. Bitte konfigurieren Sie die Anwendung neu, indem Sie ein gültiges Zertifikat angeben, oder wenden Sie sich an den Hauptadministrator.

2. Überprüfen Sie die Konfiguration des IAM-Servers und fügen Sie gegebenenfalls die Adresse des Administrationsservers zur Konfigurationsdatei des IAM-Servers hinzu.

Das klbackup-Tool verwenden, um verwaltete Geräte unter die Verwaltung eines anderen Administrationsservers zu stellen

Mit dem Tool klbackup können Sie verwaltete Geräte unter die Verwaltung eines anderen Administrationsservers stellen. Mit dem klbackup-Tool können Sie im Rahmen einer Migration vom Administrationsserver für Kaspersky Security Center Windows auf einen Administrationsserver für Kaspersky Security Center Linux wechseln. Darüber hinaus können Sie sowohl verwaltete Geräte zwischen Administrationsservern von Kaspersky Security Center Linux als auch verwaltete Geräte zwischen Administrationsservern von Kaspersky Security Center Windows migrieren.

Bevor Sie beginnen, **sehen Sie sich die Anforderungen an ein benutzerdefiniertes Zertifikat an**.

Wenn Sie anstelle des selbstsignierten Zertifikats ein benutzerdefiniertes Zertifikat verwenden, müssen Sie vor dem Upgrade von Kaspersky Security Center Linux auf die neuere Version sicherstellen, dass das Zertifikat den "Subject Alternative Name" (SAN) enthält. Wenn dies nicht der Fall ist, müssen Sie das Zertifikat unbedingt vor dem Upgrade von Kaspersky Security Center Linux ersetzen. Andernfalls können Sie sich nach dem Upgrade nicht mehr in der Webkonsole anmelden.

Um sicherzustellen, dass das Zertifikat den SAN enthält:

1. Führen Sie auf dem Gerät mit dem installierten Administrationsserver folgenden Befehl aus:

   - Für ein Linux-Gerät:

     ```
     sudo openssl x509 -in /var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer -noout
     -ext subjectAltName
     ```

   - Für ein Windows-Gerät:

     ```
     certutil -dump %ProgramData%\KasperskyLab\adminkit\1093\cert\klserver.cer
     ```

2. Stellen Sie sicher, dass der "Subject Alternative Name" in der Befehlsausgabe angezeigt wird und die Adresse des Administrationsservergeräts enthält.

3. Falls der "Subject Alternative Name" nicht angezeigt wird, verwenden Sie das Tool klsetsrvcert, um Ihr benutzerdefiniertes Zertifikat durch ein Zertifikat zu ersetzen, dass die Anforderungen erfüllt.

So stellen Sie verwaltete Geräte mit dem klbackup-Tool unter die Verwaltung eines anderen Administrationsservers:

1. Erstellen Sie auf dem bisherigen Gerät eine Backup-Kopie vom Zertifikat des Administrationsservers und von dessen privatem Schlüssel.

   Eine Backup-Kopie können Sie mit einer der folgenden Methoden erstellen:

   - Unter Verwendung des klbackup-Tools und der klbackup-Benutzeroberfläche (nur für Administrationsserver unter Kaspersky Security Center Windows)

     Starten Sie das klbackup-Tool aus dem Installationsordner von Kaspersky Security Center und legen Sie anschließend mit der Option **Nur das Zertifikat des Administrationsservers sichern und wiederherstellen** ein Backup an.

- Unter Verwendung der Eingabeaufforderung (für Administrationsserver ab Version 15.1 für Kaspersky Security Center Windows und Kaspersky Security Center Linux)

  Führen Sie das klbackup-Tool mit dem Parameter `-cert_only` über die Befehlszeile aus, um eine Backup-Kopie des Zertifikats und des privaten Schlüssels des Administrationsservers anzulegen:

  ```
  klbackup -path <Pfad zur Backup-Kopie des Administrationsserver-Zertifikats> -cert_only
  ```

2. Trennen Sie den Administrationsserver auf dem vorherigen Gerät vom Netzwerk.

3. Weisen Sie dem Gerät mit dem anderen Administrationsserver den gleichen Domänennamen zu.

   Dem neuen Administrationsserver können der NetBIOS-Name, der FQDN und die statische IP-Adresse zugewiesen werden. Dies hängt davon ab, welche Adresse für den Administrationsagenten im Installationspaket des Administrationsagenten angegeben wurde, als die Administrationsagenten verteilt wurden. Alternativ können Sie die Verbindungsadresse verwenden, die den Administrationsserver bestimmt, mit dem der Administrationsagent eine Verbindung herstellt (diese Adresse kann auf verwalteten Geräten mithilfe des Tools "klnagchk" ermittelt werden).

   Wenn es nicht möglich ist, die gleiche Adresse einem Gerät mit einem anderen Administrationsserver zuzuweisen, müssen Sie ein neues Zertifikat des Administrationsservers generieren und dieses Zertifikat in der IAM-Konfigurationsdatei angeben. Nach der Installation des Administrationsservers müssen Sie die Administrationsagenten manuell auf den neuen Administrationsserver umstellen.

4. Stellen Sie auf dem Gerät mit dem anderen Administrationsserver das Zertifikat des Administrationsservers und den privaten Schlüssel aus der Backup-Kopie wieder her.

   Eine Backup-Kopie können Sie mit einer der folgenden Methoden wiederherstellen:

   - Unter Verwendung des klbackup-Tools und der klbackup-Benutzeroberfläche (nur für Administrationsserver unter Kaspersky Security Center Windows)

     Starten Sie das klbackup-Tool und stellen Sie anschließend das Backup mithilfe der Option **Nur das Zertifikat des Administrationsservers sichern und wiederherstellen** wieder her.

   - Unter Verwendung der Eingabeaufforderung (für Administrationsserver ab Version 15.1 für Kaspersky Security Center Windows und Kaspersky Security Center Linux)

     Führen Sie das klbackup-Tool mit dem Parameter `-cert_only` über die Befehlszeile aus, um eine Backup-Kopie des Zertifikats und des privaten Schlüssels des Administrationsservers wiederherzustellen:

     ```
     klbackup -path <Pfad zur Backup-Kopie des Administrationsserver-Zertifikats> -restore -cert_only
     ```

5. Konfigurieren Sie die Überprüfung des Zertifikats durch Administrationsserver und IAM-Server.

Die verwalteten Geräte werden unter die Verwaltung eines anderen Administrationsservers gestellt. Sie können zu diesem Administrationsserver wechseln. Stellen Sie aber sicher, dass die verwalteten Geräte im Netzwerk sichtbar sind und dass der Administrationsagent auf ihnen installiert ist und ausgeführt wird (in folgenden Spalten muss der Wert auf *Yes* stehen: **Sichtbar**, **Administrationsagent ist installiert** und **Administrationsagent wird ausgeführt**).

Daten des Administrationsservers bei Verwendung von MySQL oder MariaDB sichern und wiederherstellen

Sie können ein Daten-Backup verwenden, um die Daten des Administrationsservers für Kaspersky Security Center Windows in die Verwaltung von Kaspersky Security Center Linux zu migrieren. Die Migration mittels Backups der Administrationsserver-Daten wird bei einer Migration auf Kaspersky Security Center Linux 15.2 oder höher nur für die unterstützten Versionen von Kaspersky Security Center Windows unterstützt.

Wenn Sie MySQL oder MariaDB als DBMS für Kaspersky Security Center Windows und für Kaspersky Security Center Linux verwenden, muss der Parameter `lower_case_table_names` für das aktuelle und das neue DBMS übereinstimmen. Andernfalls werden die Daten des Administrationsservers nicht korrekt migriert.

Prüfen Sie daher den Wert des Parameters `lower_case_table_names`, bevor Sie ein Backup der Daten des Administrationsservers für Kaspersky Security Center Windows anlegen. Wenn Sie diesen Parameter während der DBMS-Installation nicht angeben, wird der Standardwert des Parameters verwendet. Standardmäßig besitzt der Parameter `lower_case_table_names` unter Windows den Wert `1`.

Wenn Sie MySQL oder MariaDB für Kaspersky Security Center Linux installieren, setzen Sie den Wert des Parameters `lower_case_table_names` auf den Wert, wie er laut Anleitung von der MySQL-Website für den Parameter unter Windows vorgesehen ist. Wenn Sie diesen Parameter nicht angeben, wird der Standardwert des Parameters verwendet. Der Standardwert des Parameters `lower_case_table_names` ist für Linux-basierte Betriebssysteme und Windows verschieden.

Wenn Sie MySQL 8.0 installieren möchten, kann der Parameter `lower_case_table_names` möglicherweise nicht nach dieser Anleitung angegeben werden. In diesem Fall müssen Sie zuerst MySQL 5.7 installieren und den Parameter `lower_case_table_names` mithilfe der Anleitung angeben. Anschließend können Sie das installierte MySQL 5.7 auf MySQL 8.0 aktualisieren. Wenn der Parameter `lower_case_table_names` für das aktuelle und das neue DBMS nicht übereinstimmt, werden die Daten des Administrationsservers nicht korrekt wiederhergestellt.

Wartung des Administrationsservers

Die Wartung des Administrationsservers ermöglicht die Freigabe von Speicherplatz im Ordner des Administrationsservers und das Reduzieren der Datenbankgröße, indem nicht mehr benötigte Objekte gelöscht werden. Dies trägt zu einer verbesserten Leistung und erhöhten Ausführungszuverlässigkeit der Anwendung bei. Es wird empfohlen, den Administrationsserver mindestens einmal pro Woche zu warten.

Die Wartung des Administrationsservers erfolgt mithilfe der entsprechenden Aufgaben. Bei der Wartung des Administrationsservers führt das Programm die folgenden Aktionen aus:

- Es werden nicht benötigte Ordner und Dateien aus dem Ablageordner gelöscht.
- Es werden nicht benötigte Datensätze aus Tabellen gelöscht (auch als "hängender Zeiger" bekannt).
- Es wird der Cache geleert.

- Es wird die Datenbank gewartet (bei Verwendung von PostgreSQL als DBMS):
  - Die Datenbanken wird neu indiziert.
  - Die Datenbankstatistik wird aktualisiert.
  - Datenbank komprimieren (falls erforderlich).

Die Aufgabe Wartung des Administrationsservers unterstützt MariaDB ab Versionen 10.3. Wenn Sie MariaDB in Versionen 10.2 oder früher verwenden, müssen die Administratoren das DBMS selbst pflegen.

Die Aufgabe Wartung des Administrationsservers wird bei der Installation von Kaspersky Security Center Linux automatisch erstellt. Falls die Aufgabe Wartung des Administrationsservers gelöscht wurde, können Sie diese manuell erstellen.

So erstellen Sie die Aufgabe Wartung des Administrationsservers:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie im Fenster **Einstellungen der neue Aufgabe** des Assistenten den Aufgabentyp **Wartung des Administrationsservers** und klicken Sie auf die Schaltfläche **Weiter**.
4. Folgen Sie den weiteren Schritten des Assistenten.

Daraufhin wird die neu erstellte Aufgabe in der Aufgabenliste angezeigt. Für einen Administrationsserver kann nur eine Aufgabe des Typs Wartung des Administrationsservers ausgeführt werden. Wenn für den Administrationsserver bereits eine Aufgabe des Typs Wartung des Administrationsservers erstellt wurde, ist es nicht möglich, eine weitere Aufgabe des Typs Wartung des Administrationsservers zu erstellen.

Administrationsserver-Hierarchie löschen

Wenn Sie keine Hierarchie von Administrationsservern mehr verwenden möchten, können Sie diese von dieser Hierarchie trennen.

So löschen Sie eine Hierarchie von Administrationsservern:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.
2. Wechseln Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.
3. Wählen Sie in der Administrationsgruppe, aus der Sie den sekundären Administrationsserver löschen möchten, den entsprechenden Server aus.
4. Klicken Sie in der Menüleiste auf **Löschen**.
5. Klicken Sie im nächsten Fenster auf **OK**, um das Löschen des sekundären Administrationsservers zu bestätigen.

Der ehemalige primäre Administrationsserver und der ehemalige sekundäre Administrationsserver sind nun unabhängig voneinander. Die Hierarchie ist nicht mehr vorhanden.

Zugriff auf öffentliche DNS-Server

Wenn der Zugriff auf Kaspersky-Server über System-DNS nicht möglich ist, kann Kaspersky Security Center Linux die folgenden öffentlichen DNS-Server in der angegebenen Reihenfolge verwenden:

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

Anfragen an diese DNS-Server können Domänenadressen und die öffentliche IP-Adresse des Administrationsservers enthalten, da die Anwendung eine TCP/UDP-Verbindung zum DNS-Server herstellt. Wenn Kaspersky Security Center Linux einen öffentlichen DNS-Server verwendet, unterliegt die Datenverarbeitung der Datenschutzrichtlinie des entsprechenden Dienstes.

So konfigurieren Sie die Verwendung von öffentlichem DNS mithilfe des Tools "klscflag":

1. Öffnen Sie die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".
2. Um die Verwendung von öffentlichen DNS zu deaktivieren, führen Sie den folgenden Befehl unter einem Benutzerkonto mit Root-Berechtigung aus:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Um die Verwendung von öffentlichen DNS zu aktivieren, führen Sie den folgenden Befehl unter einem Benutzerkonto mit Root-Berechtigung aus:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Schnittstelle konfigurieren

Sie können die Benutzeroberfläche der Kaspersky Security Center Web Console so konfigurieren, dass Abschnitte und Elemente der Benutzeroberfläche abhängig von den verwendeten Funktionen ein- und ausgeblendet werden.

So konfigurieren Sie die Benutzeroberfläche der Kaspersky Security Center Web Console gemäß den derzeit verwendeten Funktionen:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Einstellungen der Benutzeroberfläche**.
2. Aktivieren oder deaktivieren Sie die erforderlichen Optionen:
   - **Verschlüsselung und Datenschutz anzeigen**
   - **Alarme von EDR anzeigen**
3. Klicken Sie auf **Speichern**.

Nachdem die erforderlichen Optionen aktiviert wurden, zeigt die Konsole die entsprechenden Abschnitte im Hauptmenü an. Wenn Sie beispielsweise **Alarme von EDR anzeigen** aktivieren, wird im Hauptmenü der Abschnitt **Überwachung** → **Alarme** angezeigt.

Geschützte Verbindung mit dem Administrationsserver einrichten

Der Datenaustausch zwischen Client-Geräten und Administrationsserver kann mithilfe des TLS-Protokolls (Transport Layer Security) erfolgen. Das TLS-Protokoll identifiziert die miteinander agierenden Seiten, führt eine Verschlüsselung der Datenübertragung durch und schützt sie vor Veränderungen bei der Übertragung. Das TLS-Protokoll basiert auf der Authentifizierung der miteinander agierenden Stellen und die Datenverschlüsselung mit offenen Schlüsseln.

Beim ersten Verbindungsaufbau zwischen einem Client-Gerät und dem Administrationsserver, empfängt der Administrationsagent auf dem Gerät eine Kopie des Zertifikats des Administrationsservers und speichert sie lokal.

Bei einer lokalen Installation des Administrationsagenten auf einem Gerät können Sie das Zertifikat des Administrationsservers manuell wählen.

Anhand der empfangenen Zertifikatskopie werden die Berechtigungen und Rechte des Administrationsservers bei den nachfolgenden Verbindungen überprüft.

Zusätzlich fragt der Administrationsagent bei jeder Verbindung des Geräts mit dem Administrationsserver das Zertifikat des Administrationsservers ab und vergleicht es mit der lokalen Kopie. Wenn sie nicht übereinstimmen, kann der Administrationsserver nicht auf das Gerät zugreifen.

Kommunikation mit TLS verschlüsseln

Um Schwachstellen im Unternehmensnetzwerk Ihres Unternehmens zu beheben, können Sie die Datenverkehrsverschlüsselung mittels TLS-Protokoll aktivieren. Sie können die TLS-Verschlüsselungsprotokolle und die unterstützten Cipher-Suites auf dem Administrationsserver aktivieren. Kaspersky Security Center Linux unterstützt das TLS-Protokoll folgender Versionen: 1.0, 1.1, 1.2 und 1.3. Sie können die erforderlichen Verschlüsselungsprotokolle und Cipher-Suites auswählen.

Kaspersky Security Center Linux verwendet selbstsignierte Zertifikate. Sie können auch Ihre eigenen Zertifikate verwenden. Die Experten von Kaspersky empfehlen, Zertifikate zu verwenden, die von vertrauenswürdigen Zertifizierungsstellen erteilt wurden.

So konfigurieren Sie die erlaubten Verschlüsselungsprotokolle und Cipher-Suites auf dem Administrationsserver:

1. Öffnen Sie die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

2. Verwenden Sie das Flag "SrvUseStrictSslSettings", um erlaubte Verschlüsselungsprotokolle und Cipher-Suites auf dem Administrationsserver zu konfigurieren. Führen Sie in der Befehlszeile den folgenden Befehl unter einem Benutzerkonto mit Root-Rechten aus:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <Wert> -t d
   ```

   Geben Sie den Parameter "<Wert>" des Flags "SrvUseStrictSslSettings" an:

   - `4` – Es sind nur die Protokolle TLS 1.2 und TLS 1.3 aktiviert. Außerdem sind Cipher-Suites mit TLS_RSA_WITH_AES_256_GCM_SHA384 aktiviert (Diese Cipher-Suites werden für die Abwärtskompatibilität mit früheren Versionen von Kaspersky Security Center Linux benötigt). Dies ist der Standardwert.

     Für das Protokoll TLS 1.2 unterstützte Cipher-Suites:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (Cipher-Suite mit TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Für das Protokoll TLS 1.3 unterstützte Cipher-Suites:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - `5` – Es sind nur die Protokolle TLS 1.2 und TLS 1.3 aktiviert. Für die Protokolle TLS 1.2 und TLS 1.3 werden die unten aufgeführten Cipher-Suites unterstützt.

     Für das Protokoll TLS 1.2 unterstützte Cipher-Suites:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

Für das Protokoll TLS 1.3 unterstützte Cipher-Suites:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Es wird nicht empfohlen, "0", "1", "2" oder "3" als Parameterwert für das Flag "SrvUseStrictSslSettings" zu verwenden. Diese Parameterwerte stehen für unsichere Versionen des TLS-Protokolls (TLS 1.0 und TLS 1.1) und unsichere Cipher-Suites. Sie werden nur aus Gründen der Abwärtskompatibilität mit älteren Versionen von Kaspersky Security Center verwendet.

3. Starten Sie die folgenden Dienste von Kaspersky Security Center Linux neu:
   - Administrationsserver
   - Webserver
   - Aktivierungs-Proxy

Dies aktiviert die Verschlüsselung des Datenverkehrs mithilfe des TLS-Protokolls.

Sie können die Flags "KLTR_TLS12_ENABLED" und "KLTR_TLS13_ENABLED" verwenden, um die Unterstützung der Protokolle TLS 1.2 bzw. TLS 1.3 zu aktivieren. Diese Flags sind standardmäßig aktiviert.

So aktivieren oder deaktivieren Sie die Unterstützung der Protokolle TLS 1.2 und TLS 1.3:

1. Führen Sie das Tool "klscflag" aus.

   Öffnen Sie die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

2. Führen Sie in der Befehlszeile einen der folgenden Befehle unter einem Benutzerkonto mit Root-Rechten aus:
   - Verwenden Sie diesen Befehl, um die Unterstützung des Protokolls TLS 1.2 zu aktivieren oder zu deaktivieren:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <Wert> -t d
     ```

   - Verwenden Sie diesen Befehl, um die Unterstützung des Protokolls TLS 1.3 zu aktivieren oder zu deaktivieren:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <Wert> -t d
     ```

   Geben Sie den Parameter `<Wert>` des Flags an:

   - `1` – Die Unterstützung des TLS-Protokolls ist aktiviert.
   - `0` – Die Unterstützung des TLS-Protokolls ist deaktiviert.

Netzwerkeinstellungen zur Interaktion mit externen Diensten

Kaspersky Security Center Linux verwendet die folgenden Netzwerkeinstellungen zur Interaktion mit externen Diensten.

Netzwerkeinstellungen

Netzwerkeinstellungen	Adresse	Beschreibung
Port: 443 Protokoll: HTTPS	`https://activation-v2.kaspersky.com`	Aktivieren des Programms

Port: 443
Protokoll: HTTPS
	`https://s00.upd.kaspersky.com`
	`https://s01.upd.kaspersky.com`
	`https://s02.upd.kaspersky.com`
	`https://s03.upd.kaspersky.com`
	`https://s04.upd.kaspersky.com`
	`https://s05.upd.kaspersky.com`
	`https://s06.upd.kaspersky.com`
	`https://s07.upd.kaspersky.com`
	`https://s08.upd.kaspersky.com`
	`https://s09.upd.kaspersky.com`
	`https://s10.upd.kaspersky.com`
	`https://s11.upd.kaspersky.com`
	`https://s12.upd.kaspersky.com`
	`https://s13.upd.kaspersky.com`
	`https://s14.upd.kaspersky.com`
	`https://s15.upd.kaspersky.com`
	`https://s16.upd.kaspersky.com`
	`https://s17.upd.kaspersky.com`
	`https://s18.upd.kaspersky.com`
	`https://s19.upd.kaspersky.com`
	`https://cm.k.kaspersky-labs.com`
		Aktualisieren der Datenbanken, Softwaremodule und Anwendungen von Kaspersky

Port: 443 Protokoll: HTTPS	`https://downloads.upd.kaspersky.com`	• Aktualisieren der Datenbanken, Softwaremodule und Anwendungen von Kaspersky • Es wird geprüft, ob auf die Kaspersky-Server zugegriffen werden kann. Vor dem Herunterladen von Kaspersky-Datenbanken und Softwaremodulen überprüft Kaspersky Security Center Linux, ob die Kaspersky-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server.

Netzwerkeinstellungen	Adresse	Beschreibung
Port: 80 Protokoll: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Aktualisieren der Datenbanken, Softwaremodule und Anwendungen von Kaspersky
Port: 443 Protokoll: HTTPS	https://ds.kaspersky.com https://dc1.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com/ https://dc1-cert.ksn.kaspersky-labs.com https://dc1-cf.ksn.kaspersky-labs.com https://dc1-file.ksn.kaspersky-labs.com https://dc1-kas.ksn.kaspersky-labs.com https://dc1-ml.ksn.kaspersky-labs.com https://dc1-pp.ksn.kaspersky-labs.com https://dc1-st.ksn.kaspersky-labs.com https://dc1.ksn.kaspersky-labs.com	Verwenden von Kaspersky Security Network

Netzwerkeinstellungen	Adresse	Beschreibung

Port: 443, 1443
Protokoll: HTTPS
	`https://ksn-file-geo.kaspersky-labs.com`
	`https://ksn-verdict-geo.kaspersky-labs.com`
	`https://ksn-url-geo.kaspersky-labs.com`
	`https://ksn-a-p2p-geo.kaspersky-labs.com`
	`https://ksn-info-geo.kaspersky-labs.com`
	`https://ksn-cinfo-geo.kaspersky-labs.com`
		Verwenden von Kaspersky Security Network

Port: 443, 1443
Protokoll: KSN
	`ksn://ksn-a-p2p-geo.kaspersky-labs.com`
	`ksn://ksn-a-stat-geo.kaspersky-labs.com`
	`ksn://ksn-ca-geo.kaspersky-labs.com`
	`ksn://ksn-cinfo-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-catm-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-dnscheck-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-hash-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-ipm-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-whocalls-geo.kaspersky-labs.com`
	`ksn://ksn-crypto-wifiplus-geo.kaspersky-labs.com`
	`ksn://ksn-eu-stat-kmp.kaspersky-labs.com`
	`ksn://ksn-file-geo.kaspersky-labs.com`
	`ksn://ksn-his-geo.kaspersky-labs.com`
	`ksn://ksn-info-geo.kaspersky-labs.com`
	`ksn://ksn-kas-geo.kaspersky-labs.com`
	`ksn://ksn-kddi.kaspersky-labs.com`
	`ksn://ksn-ml-geo.kaspersky-labs.com`
	`ksn://ksn-oui-geo.kaspersky-labs.com`
	`ksn://ksn-pp.kaspersky-labs.com`
	`ksn://ksn-src.kaspersky-labs.com`
	`ksn://ksn-stat-geo.kaspersky-labs.com`
	`ksn://ksn-tcert-geo.kaspersky-labs.com`
	`ksn://ksn-url-geo.kaspersky-labs.com`
	`ksn://ksn-verdict-geo.kaspersky-labs.com`
	`ksn://mdr.ksn.kaspersky-labs.com`
	`ksn://stat-eu.ksn.kaspersky-labs.com`
	`ksn://stat-hq.ksn.kaspersky-labs.com`
	`ksn://stat-ru.ksn.kaspersky-labs.com`
	`ksn://stat-sa.ksn.kaspersky-labs.com`
	`ksn://stat-sbr.ksn.kaspersky-labs.com`
		Verwenden von Kaspersky Security Network

Port: 443 Protokoll: HTTPS	`https://click.kaspersky.com` `https://redirect.kaspersky.com`	Folgen von Links aus der Benutzeroberfläche

Netzwerkeinstellungen	Adresse	Beschreibung
Port: 80 Protokoll: HTTP	`http://crl.kaspersky.com` `http://ocsp.kaspersky.com`	Diese Server sind Teil der Public Key Infrastructure (PKI) und werden benötigt, um die Gültigkeit der Zertifikate mit den digitalen Signaturen von Kaspersky zu überprüfen. Die CRL ist eine Liste mit Zertifikaten, die widerrufen wurden. Mittels OCSP können Sie den Status eines bestimmten Zertifikats in Echtzeit abfragen. Diese Server erhöhen die Sicherheit bei der Interaktion mit digitalen Zertifikaten und schützen vor möglichen Angriffen.
Port: 443 Protokoll: HTTPS	`https://ipm-klca.kaspersky.com`	Marketing-Mitteilungen
Port: 443 Protokoll: HTTPS	`https://tip.kaspersky.com`	Mittels Kaspersky Threat Intelligence Portal auf Bedrohungen reagieren (bei Verwendung der Funktionalitäten von Kaspersky Next XDR Optimum).
Port: 443 Protokoll: HTTPS	Eine vollständige Liste der Adressen finden Sie im Artikel Adresse und Domainstruktur.	Mittels Kaspersky Automated Security Awareness Platform reagieren (bei Verwendung der Funktionalitäten von Kaspersky Next XDR Optimum).

Berücksichtigen Sie die folgenden Empfehlungen, damit Kaspersky Security Center Linux ordnungsgemäß mit externen Diensten interagiert:
- Auf den Netzwerkgeräten und dem Proxyserver Ihres Unternehmens muss auf den Ports 443 und 1443 unverschlüsselter Netzwerkdatenverkehr erlaubt sein.
- Wenn der Administrationsserver mit den Kaspersky-Update-Servern und den Servern von Kaspersky Security Network interagiert, muss verhindert werden, dass der Netzwerkdatenverkehr durch das Ersetzen von Zertifikaten übernommen wird (MITM-Angriffe).

So laden Sie mit dem Tool "klscflag" Updates über das HTTP- oder HTTPS-Protokoll herunter:

1. Öffnen Sie die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

2. Wenn Sie Updates über das HTTP-Protokoll herunterladen möchten, führen Sie einen der folgenden Befehle unter einem Benutzerkonto mit Root-Rechten aus:

   - Auf dem Gerät mit installiertem Administrationsserver:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - Auf einem Verteilungspunkt:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Wenn Sie Updates über das HTTPS-Protokoll herunterladen möchten, führen Sie einen der folgenden Befehle unter einem Benutzerkonto mit Root-Rechten aus:

   - Auf dem Gerät mit installiertem Administrationsserver:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - Auf einem Verteilungspunkt:

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Globale Liste der Subnetze

Für jeden von Ihnen verwendeten Administrationsserver können Sie eine globale Liste mit Subnetzen einrichten, um die Informationen über die Subnetz in Ihrem Netzwerk zu speichern. Diese Liste hilft Ihnen dabei Paare {IP-Adresse, Maske} und physikalische Einheiten wie Filialen übereinzustimmen. Sie können Subnetze aus dieser Liste in den Netzwerkregeln und Einstellungen verwenden.

Um ein Subnetz zur globalen Liste der Subnetze hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Globale Subnetze** aus.

3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Neues Subnetz** wird geöffnet.

4. Füllen Sie die folgenden Felder aus:

   - **Name**
   - **Subnetzadresse**
   - **Subnetzmaske**
   - **Beschreibung**

5. Klicken Sie auf die Schaltfläche **Speichern**.

Das Fenster wird geschlossen und das Subnetz erscheint in der Liste der Subnetze.

Bei Bedarf können Sie in der Liste der globalen Subnetze Folgendes tun:

- Subnetze aus der Liste löschen, indem Sie das gewünschte Subnetz auswählen und auf die Schaltfläche **Entfernen** klicken.
- Ändern Sie die Eigenschaften von Subnetzen, indem Sie auf den Link mit dem Namen des gewünschten Subnetzes klicken und anschließend die in den Schritten 4 bis 5 beschriebenen Aktionen ausführen.

Integrität der Module anhand der Tools klscmodchk und integrity_checker prüfen

Kaspersky Security Center Linux enthält mehrere Binärmodule in Form von dynamisch verlinkten Bibliotheken, ausführbaren Dateien, Konfigurationsdateien und Schnittstellendateien. Eindringlinge können eine oder mehrere ausführbare Dateien oder Anwendungsdateien durch Dateien mit schädlichem Code ersetzen. Um das Ersetzen von Modulen oder Dateien zu verhindern, bietet Kaspersky Security Center Linux mit den Tools "klscmodchk" und "integrity_checker" eine Integritätsprüfung für Komponenten. Diese Tools prüfen Module und Dateien auf unbefugte Änderungen oder Beschädigungen. Wenn die Prüfsumme eines Moduls oder einer Anwendung nicht korrekt ist, gilt das Modul oder die Anwendung als beschädigt.

Das Tool "klscmodchk" führt die Integritätsprüfungen für die folgenden Komponenten von Kaspersky Security Center Linux durch:

- Administrationsserver
- Administrationsagent

Das Tool "integrity_checker" führt die Integritätsprüfungen für die folgenden Komponenten von Kaspersky Security Center Linux durch:

- Administrationsserver
- Administrationsagent
- Kaspersky Security Center Web Console

Beide Tools prüfen die Integrität auf Grundlage der Manifest-Datei "kl_file_integrity_manifest.xml", die ein Teil der Build-Version von Kaspersky Security Center Linux ist und sich im Installationsordner befindet. Die Komponenten-Manifest-Datei enthält Dateien, deren Integrität für den ordnungsgemäßen Betrieb von Kaspersky Security Center Linux wichtig ist. Die Integrität der Manifest-Dateien wird ebenfalls geprüft.

Es wird dringend empfohlen, die Manifest-Datei "kl_file_integrity_manifest.xml" nicht zu verändern, da dies die digitalen Signaturen ungültig macht und die Integritätsprüfung fehlschlagen lässt.

Um die Integrität von Kaspersky Security Center Linux zu prüfen, führen Sie einen der folgenden Befehle aus:

- `$ klscmodchk [ Parameter ]`

  Das Tool "klscmodchk" startet das Tool "integrity_checker" mit dem Parameter `--verbose` und prüft die Integrität der Module.

  Parameter des Tools "klscmodchk":

  - `-logfile < Pfad_der_Protokolldatei >` – Geben Sie zum Protokollieren einen Dateipfad auf der Festplatte an. Standardmäßig erfolgt die Ausgabe über die Konsole.
  - `-verbose` – Ausgeben von erweiterten Informationen während der Integritätsprüfung.

- `$ integrity_checker [ Parameter ] < Pfad_zur_Manifest-Datei >`

Parameter des Tools "integrity_checker":

- `--help` – Anzeigen der Hilfe des Tools "integrity_checker".
- `--version` – Anzeigen der Versionsnummer des Tools "integrity_checker".
- `--verbose` – Anzeigen von Informationen zur Ausführung des Tools. Bei der Durchführung einer Integritätsprüfung ist es ausreichend, diesen Parameter im Befehl zu verwenden.

Das Ergebnis der Prüfung wird für jede Manifest-Datei neben ihrem Namen im folgenden Format angezeigt:

- SUCCEEDED – Die Integrität der Datei wurde bestätigt (Rückgabe-Code 0).
- FAILED – Die Integrität der Datei wurde nicht bestätigt (Rückgabe-Code von null abweichend).

Sie können Integritätsprüfungen auch so konfigurieren, dass sie automatisch gestartet werden, wenn Sie die Anwendung starten. Standardmäßig ist die automatische Integritätsprüfung deaktiviert.

So aktivieren Sie die automatische Integritätsprüfung:

1. Geben Sie auf dem Gerät mit dem installierten Administrationsserver in der Befehlszeile den folgenden Befehl ein:

   ```
   ./klscflag -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Starten Sie das Gerät neu.

   Die automatische Integritätsprüfung ist aktiviert.

Beim nächsten Start von Kaspersky Security Center wird das Tool "klscmodchk" zusammen mit dem Administrationsserver ausgeführt und startet die Integritätsprüfung der Module. Die Ergebnisse der Integritätsprüfungen werden in das Kaspersky-Ereignisprotokoll geschrieben.

Geräte im Netzwerk finden

In diesem Abschnitt wird die Suche und Entdeckung von Geräten im Netzwerk beschrieben.

Kaspersky Security Center Linux ermöglicht eine Suche der Geräte auf der Grundlage der angegebenen Kriterien. Sie können Suchergebnisse in einer Textdatei speichern.

Mit der Such- und Ermittlungsfunktion können folgende Geräte gefunden werden:

- Verwaltete Geräte der Administrationsgruppen des Kaspersky Security Center Administrationsservers und seiner sekundären Administrationsserver.
- Nicht zugeordnete Geräte, die vom Kaspersky Security Center Administrationsservers und seiner sekundären Administrationsserver verwaltet werden.

Szenario: Netzwerkgeräte finden

Die Gerätesuche muss vor der Installation einer Sicherheitsanwendung ausgeführt werden. Sobald alle Geräte im Netzwerk gefunden wurden, können Sie Informationen zu diesen Geräten abrufen und sie mithilfe von Richtlinien verwalten. Regelmäßige Netzwerkabfragen sind nötig, um neue Geräte im Netzwerk zu erkennen und zu prüfen, ob die bereits erkannten Geräte sich noch im Netzwerk befinden.

Das Erkennen von Geräten im Netzwerk erfolgt in mehreren Etappen:

1. **Erstmalige Gerätesuche**

   Führen Sie nach Abschluss des Schnellstartassistenten die Gerätesuche manuell aus.

2. **Zukünftige Abfragen konfigurieren**

   Stellen Sie sicher, dass IP-Bereiche durchsuchen aktiviert ist und dass der Abfragezeitplan die Anforderungen Ihres Unternehmens erfüllt. Verwenden Sie bei der Konfiguration des Abfragezeitplans die Empfehlungen zur Häufigkeit der Netzwerkabfrage.

   Sie können auch Zeroconf-Abfragen aktivieren, wenn Ihr Netzwerk IPv6-Geräte enthält.

   Wenn Netzwerkgeräte zu einer Domäne gehören, wird es empfohlen, die Abfrage des Domänencontrollers zu verwenden.

   Verwenden Sie stattdessen Windows-basierte Verteilungspunkte, um Windows-Netzwerke abzufragen.

3. **Regeln zum Hinzufügen neu entdeckter Geräte zu Administrationsgruppen einrichten (optional)**

   Wenn in Ihrem Netzwerk neue Geräte auftauchen, werden sie bei regelmäßigen Abfragen entdeckt und automatisch zur Gruppe **Nicht zugeordnete Geräte** hinzugefügt. Bei Bedarf können Sie die Regeln so einrichten, dass diese Geräte automatisch zur Gruppe **Verwaltete Geräte** verschoben werden. Darüber hinaus können Sie Aufbewahrungsregeln einrichten.

   Wenn Sie diesen Schritt der Regelerstellung überspringen, werden alle neu entdeckten Geräte zur Gruppe **Nicht zugeordnete Geräte** hinzugefügt und bleiben dort. Bei Bedarf können Sie diese Geräte manuell in die Gruppe **Verwaltete Geräte** verschieben. Wenn Sie die Geräte manuell in die Gruppe **Verwaltete Geräte** verschieben, können Sie die Informationen zu jedem Gerät analysieren, bestimmen, ob das Gerät in eine Administrationsgruppe verschoben werden soll, und die entsprechende Gruppe wählen.

Ergebnisse

Der Abschluss des Szenarios bringt folgende Ergebnisse mit sich:

- Der Kaspersky Security Center Linux Administrationsserver findet die Geräte im Netzwerk und stellt Ihnen Informationen zu diesen Geräten zur Verfügung.
- Zukünftige Abfragen werden eingerichtet und nach einem festgelegten Zeitplan ausgeführt.

Neu entdeckte Geräte werden gemäß den konfigurierten Regeln bestimmten Gruppen zugewiesen. (Falls keine Regeln erstellt wurden, bleiben die Geräte in der Gruppe **Nicht zugeordnete Geräte**).

Windows-Netzwerkabfrage

Über die Windows-Netzwerkabfrage

Kaspersky Security Center Linux unterstützt keine Windows-Netzwerkabfrage. Verwenden Sie stattdessen Windows-basierte Verteilungspunkte, um Windows-Netzwerke abzufragen.

Bei der Schnellabfrage rufen Verteilungspunkte nur Informationen über die Liste der NetBIOS-Namen der Geräte aller Domänen und Arbeitsgruppen des Netzwerks ab. Bei einer vollständigen Abfrage werden von jedem Client-Gerät folgende Informationen angefordert:

- Betriebssystem-Name
- IP-Adresse
- DNS-Name
- NetBIOS-Name

Die folgenden Voraussetzungen gelten sowohl für die schnelle als auch für die vollständige Abfrage:

- Die Ports UDP 137/138, TCP 139, UDP 445, TCP 445 müssen im Netzwerk verfügbar sein.
- Das SMB-Protokoll ist aktiviert.
- Der Microsoft-Computersuchdienst muss verwendet werden, und der Computer mit dem primären Suchdienst muss auf dem Administrationsserver aktiviert sein.
- Der Microsoft-Computersuchdienst muss verwendet werden, und der Computer mit dem primären Suchdienst muss auf den Client-Geräten aktiviert sein:
  - Auf mindestens einem Gerät, wenn sich nicht mehr als 32 Geräte im Netzwerk befinden.
  - Auf mindestens einem Gerät pro 32 Geräten im Netzwerk.

Die vollständige Abfrage kann nur durchgeführt werden, wenn die Schnellabfrage mindestens einmal durchgeführt wurde.

IP-Bereiche abfragen

Kaspersky Security Center Linux versucht für jede IPv4-Adresse aus dem festgelegten Bereich eine umgekehrte Namensauflösung zu einem DNS-Namen mithilfe von Standard-DNS-Abfragen durchzuführen. Wenn dieser Vorgang erfolgreich ist, sendet der Server einen `ICMP ECHO REQUEST` (entspricht einem ping-Befehl) an den empfangenen Namen. Wenn das Gerät antwortet, werden die Informationen darüber zur Kaspersky Security Center Linux -Datenbank hinzugefügt. Die umgekehrte Namensauflösung ist erforderlich, um Netzwerkgeräte auszuschließen, die über eine IP-Adresse verfügen können, aber keine Computer sind (Netzwerkdrucker, Router usw.).

Dieses Abfrageverfahren benötigt einen korrekt konfigurierten DNS-Dienst. Dieser muss über eine Reverse-Lookupzone verfügen. Wenn diese Zone nicht konfiguriert ist, ergibt die IP-Subnetzabfrage keine Ergebnisse.

Ursprünglich erhält Kaspersky Security Center Linux IP-Bereiche für die Abfrage aus den Netzwerk-Einstellungen des Geräts, auf dem es installiert ist. Wenn die Geräteadresse 192.168.0.1 lautet und die Subnetzmaske 255.255.255.0 ist, fügt Kaspersky Security Center Linux das Netzwerk 192.168.0.0/24 automatisch zur Liste der Abfrageadressen hinzu. Kaspersky Security Center Linux fragt alle Adressen von 192.168.0.1 bis 192.168.0.254 ab.

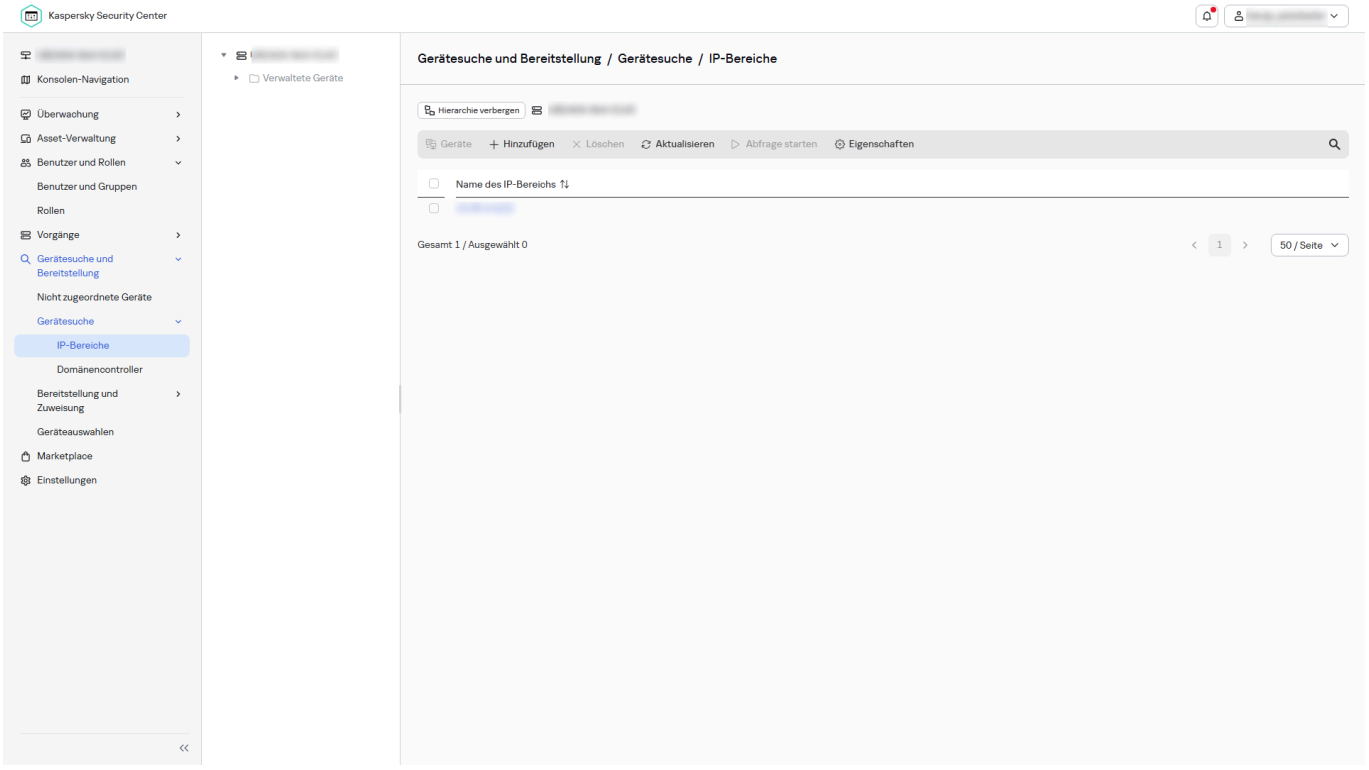
Wenn nur die IP-Bereichsabfrage aktiviert ist, erkennt Kaspersky Security Center Linux nur Geräte mit IPv4-Adressen. Wenn Ihr Netzwerk IPv6-Geräte enthält, aktivieren Sie die Zeroconf-Abfrage von Geräten.

Geben Sie für alle Linux-basierten Hosts innerhalb eines Microsoft Active Directory- oder Samba-Domänencontrollers die Parameter `netbios name` und `workgroup` in der Datei `/etc/samba/smb.conf` an. Andernfalls können Hosts mehrfach in den Abfrageergebnissen enthalten sein.

Einstellungen für die Abfrage der IP-Bereiche anzeigen und ändern

Um die Einstellungen für die Abfrage der IP-Bereiche anzuzeigen und zu ändern, gehen Sie wie folgt vor:

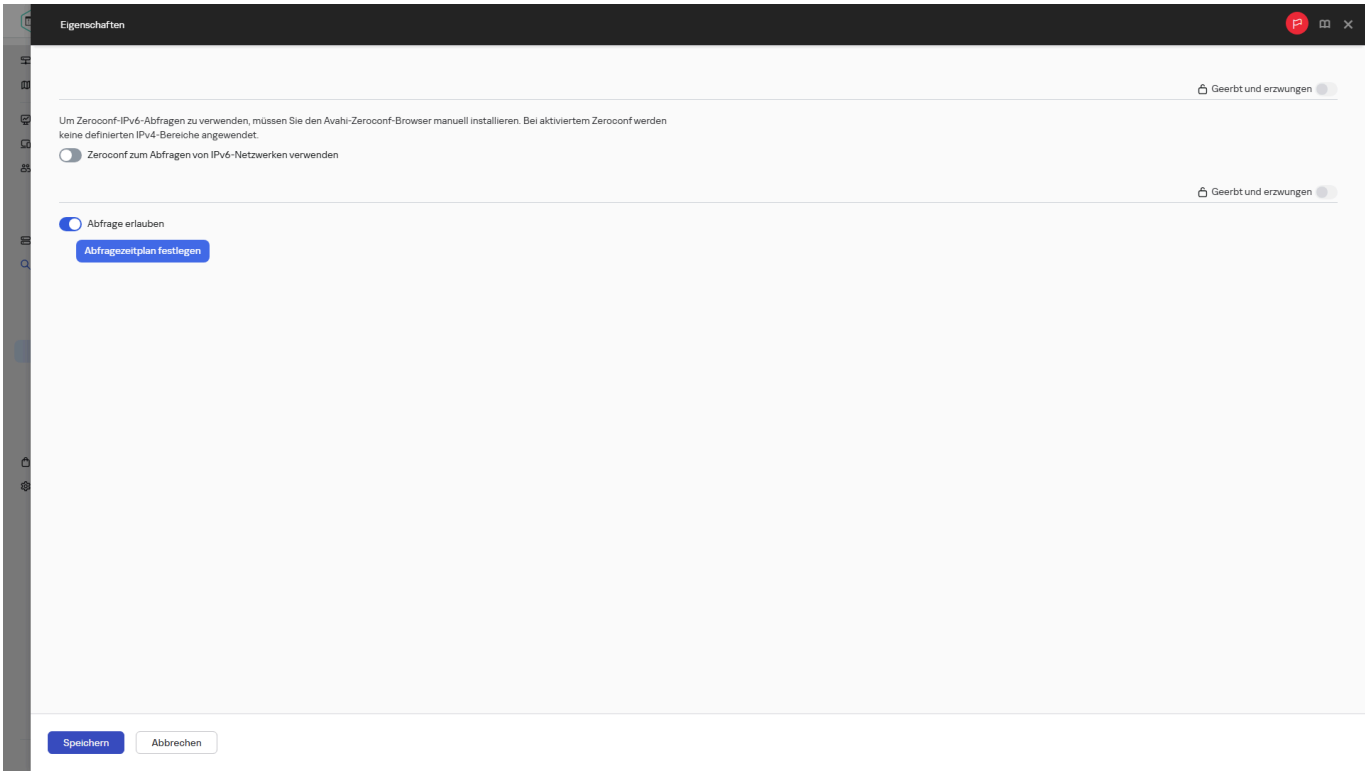
1. Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → IP-Bereiche**.



Liste der IP-Bereiche

2. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Eigenschaftenfenster der IP-Abfrage wird geöffnet.



Die Eigenschaften der IP-Abfrage

3. Aktivieren oder deaktivieren Sie die IP-Abfrage mit dem Schalter **Abfrage erlauben**.

4. Passen Sie den Abfragezeitplan an. Standardmäßig wird die IP-Abfrage alle 420 Minuten (sieben Stunden) ausgeführt.

   Achten Sie bei der Angabe des Abfrageintervalls darauf, dass diese Angabe den Wert der Lebensdauer der IP-Adresse nicht übersteigt. Wird eine IP-Adresse nicht innerhalb ihrer Lebensdauer durch eine Abfrage verifiziert, wird sie automatisch aus den Abfrageergebnissen entfernt. Standardmäßig beträgt die Lebensdauer der Abfrageergebnisse 24 Stunden, da dynamische IP-Adressen (mithilfe des DHCP-Protokolls (Dynamic Host Configuration Protocol) zugewiesen) alle 24 Stunden geändert werden.

   Varianten für den Zeitplan der Abfrage:

   - **Alle n Tage**

     Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

     Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

   - **Alle n Minuten**

     Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

   - **Nach Wochentagen**

     Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

   - **Monatlich am ausgewählten Tag**

     Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

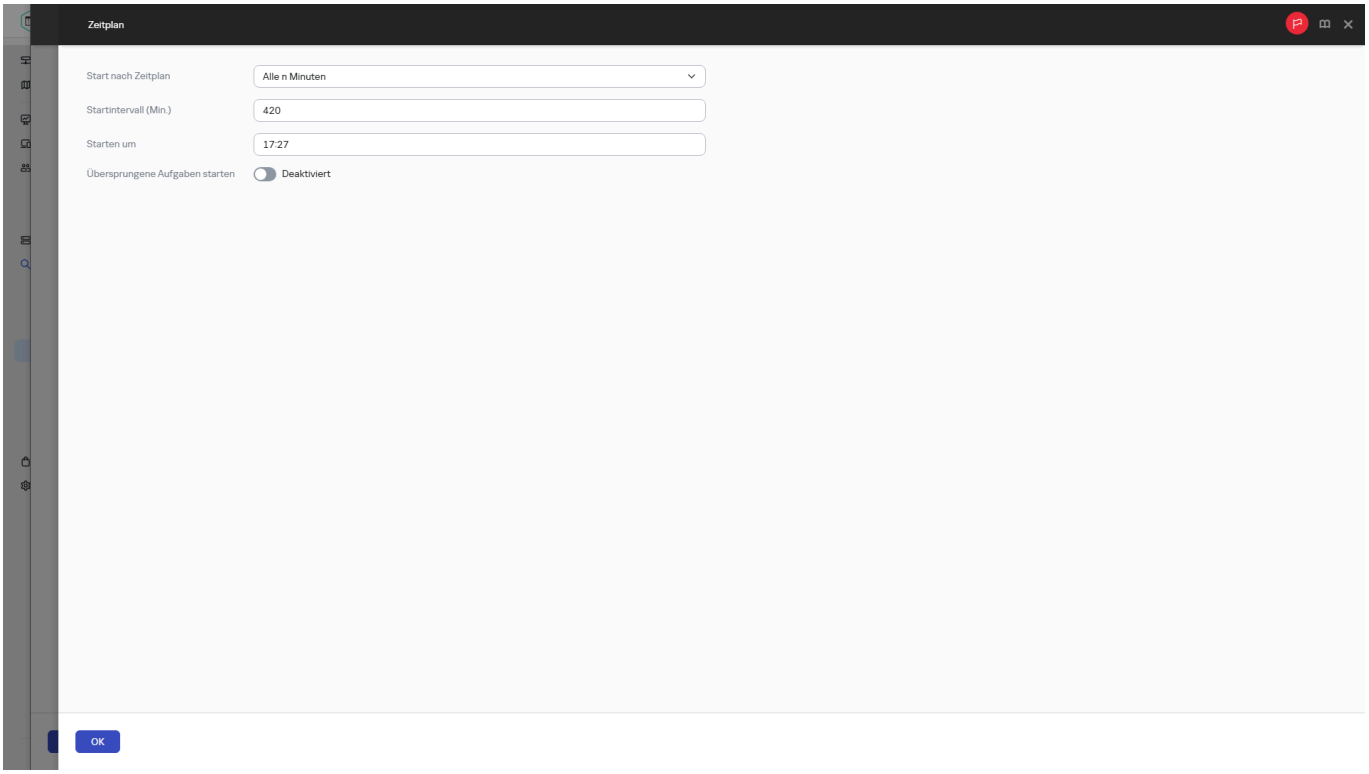
   - **Übersprungene Aufgaben starten**

     Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

     Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

     Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

Diese Option ist standardmäßig deaktiviert.



Abfragezeitplan anpassen

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Eigenschaften werden gespeichert und auf alle IP-Bereiche angewendet.

Abfrage manuell ausführen

Um die Abfrage sofort auszuführen,

Klicken Sie auf **Abfrage starten**.

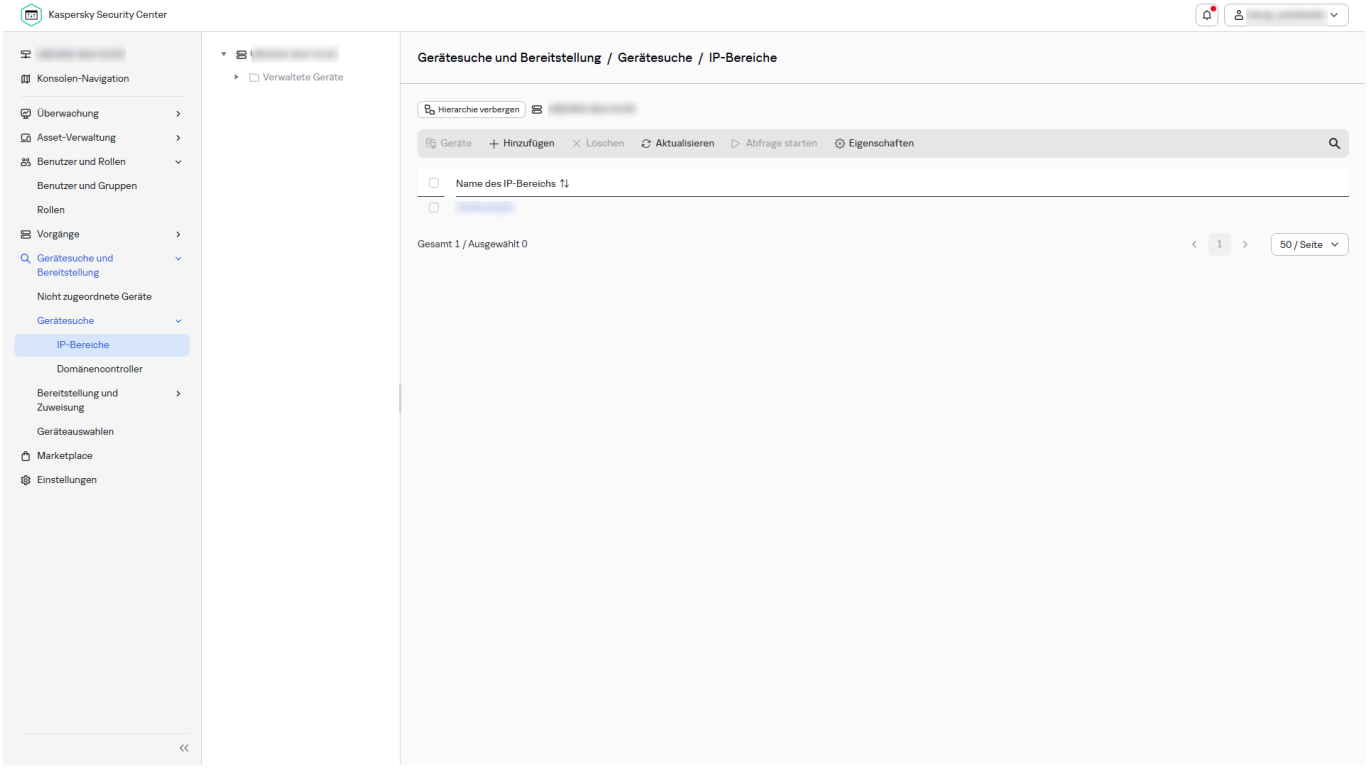
IP-Bereich hinzufügen und bearbeiten

Ursprünglich erhält Kaspersky Security Center Linux IP-Bereiche für die Abfrage aus den Netzwerk-Einstellungen des Geräts, auf dem es installiert ist. Wenn die Geräteadresse 192.168.0.1 lautet und die Subnetzmaske 255.255.255.0 ist, fügt Kaspersky Security Center Linux das Netzwerk 192.168.0.0/24 automatisch zur Liste der Abfrageadressen hinzu. Kaspersky Security Center Linux fragt alle Adressen von 192.168.0.1 bis 192.168.0.254 ab. Sie können die automatisch festgelegten IP-Bereiche bearbeiten oder eigene IP-Bereiche hinzufügen.

Bereiche können nur für IPv4-Adressen erstellt werden. Wenn Sie die Zeroconf-Abfrage aktivieren, wird Kaspersky Security Center Linux das gesamte Netzwerk abfragen.

Um einen neuen IP-Bereich hinzuzufügen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → IP-Bereiche**.



Liste der IP-Bereiche

2. Klicken Sie auf **Hinzufügen**, um den neuen IP-Bereich hinzuzufügen.

3. Passen Sie im nächsten Fenster folgende Einstellungen an:

   - **Name des IP-Bereichs**

     Der Name des IP-Bereichs. Sie können den IP-Bereich selbst als Namen angeben, z. B. "192.168.0.0/24".

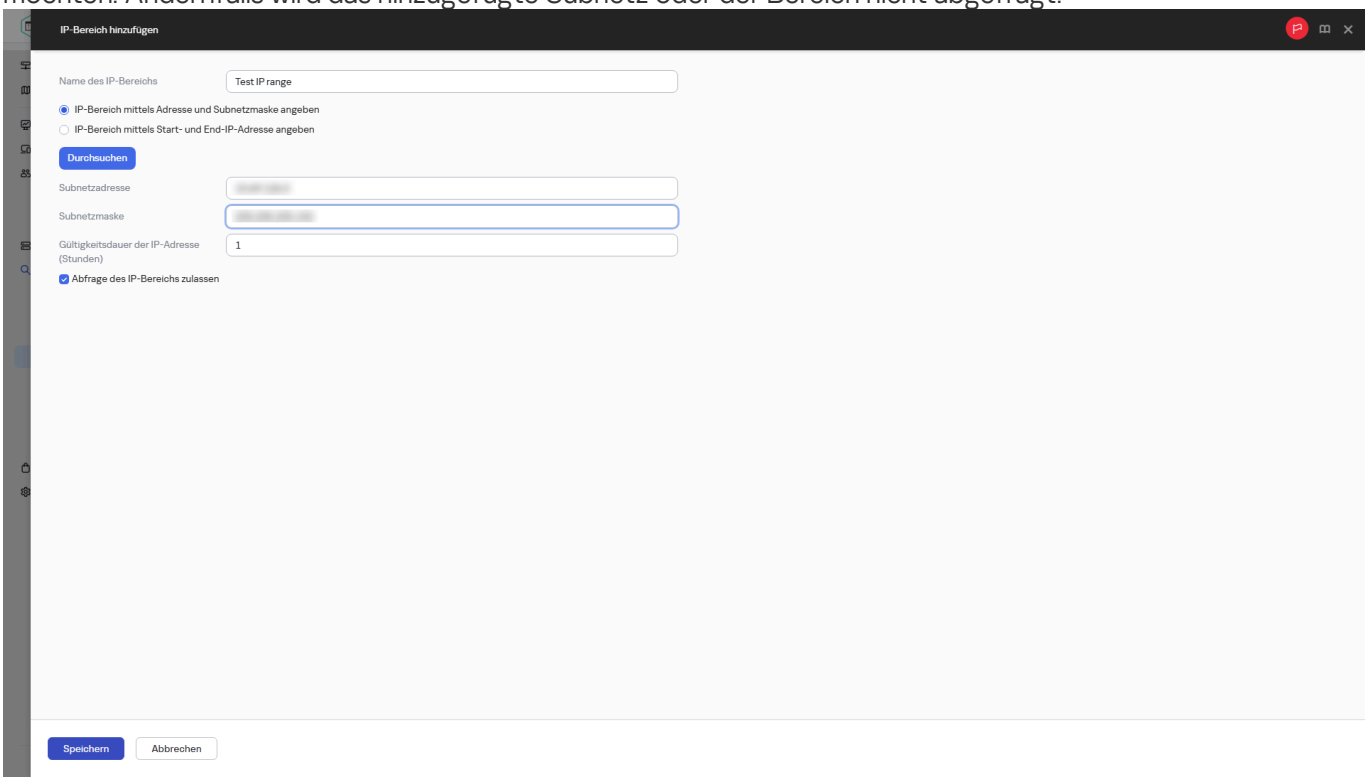
   - **IP-Intervall oder Subnetzadresse und Maske**

     Legen Sie den IP-Bereich fest, indem Sie entweder die erste und letzte IP-Adresse oder die Subnetzadresse und Subnetzmaske angeben. Sie können auch einen der bereits vorhandenen IP-Bereiche auswählen, indem Sie auf **Durchsuchen** klicken.

   - **Gültigkeitsdauer der IP-Adresse (Stunden)**

     Stellen Sie bei Angabe dieser Einstellung sicher, dass die Lebensdauer das im Abfragezeitplan festgelegte Abfrageintervall übersteigt. Wird eine IP-Adresse nicht innerhalb ihrer Lebensdauer durch eine Abfrage verifiziert, wird sie automatisch aus den Abfrageergebnissen entfernt. Standardmäßig beträgt die Lebensdauer der Abfrageergebnisse 24 Stunden, da dynamische IP-Adressen (mithilfe des DHCP-Protokolls (Dynamic Host Configuration Protocol) zugewiesen) alle 24 Stunden geändert werden.

4. Wählen Sie **Abfrage des IP-Bereichs zulassen**, wenn Sie das hinzugefügte Subnetz oder den Bereich abfragen möchten. Andernfalls wird das hinzugefügte Subnetz oder der Bereich nicht abgefragt.



Konfiguration der Einstellungen für den IP-Bereich

5. Klicken Sie auf die Schaltfläche **Speichern**.

   Der neue IP-Bereich wird zur Liste mit IP-Bereichen hinzugefügt.

Sie können jeden IP-Bereich separat durchsuchen, indem Sie auf **Abfrage starten** klicken. Standardmäßig beträgt die Lebensdauer der Abfrageergebnisse 24 Stunden und entspricht der festgelegten Lebensdauer der IP-Adresse.

Um eine neues Subnetz zu einem vorhandenen IP-Bereich hinzuzufügen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → IP-Bereiche**.

2. Klicken Sie auf den Namen des IP-Bereichs, zu dem Sie ein Subnetz hinzufügen möchten.

3. Klicken Sie im folgenden Fenster auf **Hinzufügen**.

4. Geben Sie ein Subnetz an, indem Sie entweder dessen Adresse und Maske oder die erste und letzte IP-Adresse im IP-Bereich verwenden. Sie können auch ein vorhandenes Subnetz hinzufügen, indem Sie auf **Durchsuchen** klicken.

5. Klicken Sie auf die Schaltfläche **Speichern**.

   Das neue Subnetz wird zum IP-Bereich hinzugefügt.

6. Klicken Sie auf die Schaltfläche **Speichern**.

   Die neuen Einstellungen des IP-Bereichs werden gespeichert.

Sie können beliebig viele Subnetze hinzufügen. Benannte IP-Bereiche dürfen sich nicht überlappen, aber für unbenannte Subnetze innerhalb eines IP-Bereichs gilt keine derartige Beschränkung. Sie können die Abfrage für jeden IP-Bereich unabhängig aktivieren und deaktivieren.

Zeroconf-Abfrage

Diese Art der Abfrage wird nur von Linux-basierten Verteilungspunkten unterstützt.

Kaspersky Security Center Linux kann Netzwerke abfragen, die Geräte mit IPv6-Adressen enthalten. In diesem Fall werden keine IP-Bereiche angegeben, und Kaspersky Security Center Linux fragt das gesamte Netzwerk unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) ab. Um mit der Verwendung von Zeroconf zu beginnen, müssen Sie das Dienstprogramm avahi-browse auf dem Linux-Gerät installieren, das Netzwerke abfragt, also auf dem Administrationsserver oder einem Verteilungspunkt.

So aktivieren Sie die Zeroconf-Abfrage:

1. Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → IP-Bereiche**.
2. Klicken Sie auf die Schaltfläche **Eigenschaften**.
3. Aktivieren Sie im angezeigten Fenster die Umschaltfläche **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden**.

Danach beginnt Kaspersky Security Center Linux das Netzwerk abzufragen. In diesem Fall werden die angegeben IP-Bereiche ignoriert.

Abfrage des Domänencontrollers

Kaspersky Security Center Linux unterstützt die Abfrage der folgenden Typen von Domänencontrollern:

- Microsoft Active Directory
- Samba
- FreeIPA
- ALD Pro

Für einen Samba-Domänencontroller wird Samba 4 als Active Directory-Domänencontroller verwendet.

Wenn Sie einen Domänencontroller abfragen, ruft der Administrationsserver oder ein Verteilungspunkt Informationen über die Domänenstruktur, Benutzerkonten, Sicherheitsgruppen und DNS-Namen jener Geräte ab, die zur Domäne gehören.

Es wird empfohlen, die Abfrage von Domänencontrollern zu verwenden, wenn alle Geräte im Netzwerk Mitglieder einer Domäne sind. Wenn einige der vernetzten Geräte nicht in der Domäne enthalten sind, können diese Geräte mit der Abfrage des Domänencontrollers nicht gefunden werden.

Während der Abfrage eines Microsoft Active Directory sendet der Server ICMP-Echo-Anfragen (entspricht dem Befehl "ping").

Erforderliche Voraussetzungen

Stellen Sie vor der Abfrage eines Domänencontrollers sicher, dass Sie Verbindungen mit dem Domänencontroller durch eine Firewall oder einen Proxyserver zulassen. Stellen Sie außerdem sicher, dass die folgenden Protokolle auf dem Domänencontroller aktiviert sind:

- Lightweight Directory Access Protocol (LDAP)
- Simple Authentication and Security Layer (SASL)

  Dieses Protokoll wird verwendet, wenn die Verbindung zum Domänencontroller mithilfe der SASL-Authentifizierung hergestellt wird. Der Administrationsserver und die Verteilungspunkte unterstützen nur den Mechanismus DIGEST-MD5.
- Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS)

  Dieses Protokoll wird verwendet, wenn Sie eine verschlüsselte Verbindung zum Domänencontroller herstellen müssen.

Stellen Sie sicher, dass auf dem Gerät des Domänencontrollers die folgenden Ports verfügbar sind:

- 389 für das LDAP-Protokoll und Simple Authentication (einschließlich SASL)
- 636 für das LDAPS-Protokoll

Für FreeIPA und ALD Pro werden die LDAP- und LDAPS-Protokolle nur für die Domänenabfrage verwendet. Kaspersky Security Center Linux unterstützt die Authentifizierung von FreeIPA-Benutzerkonten über LDAP bzw. LDAPS nicht. Damit sich FreeIPA- und ALD Pro-Benutzer an der Web Console anmelden können, müssen Sie die Kerberos-Authentifizierung über den IAM-Dienst konfigurieren.

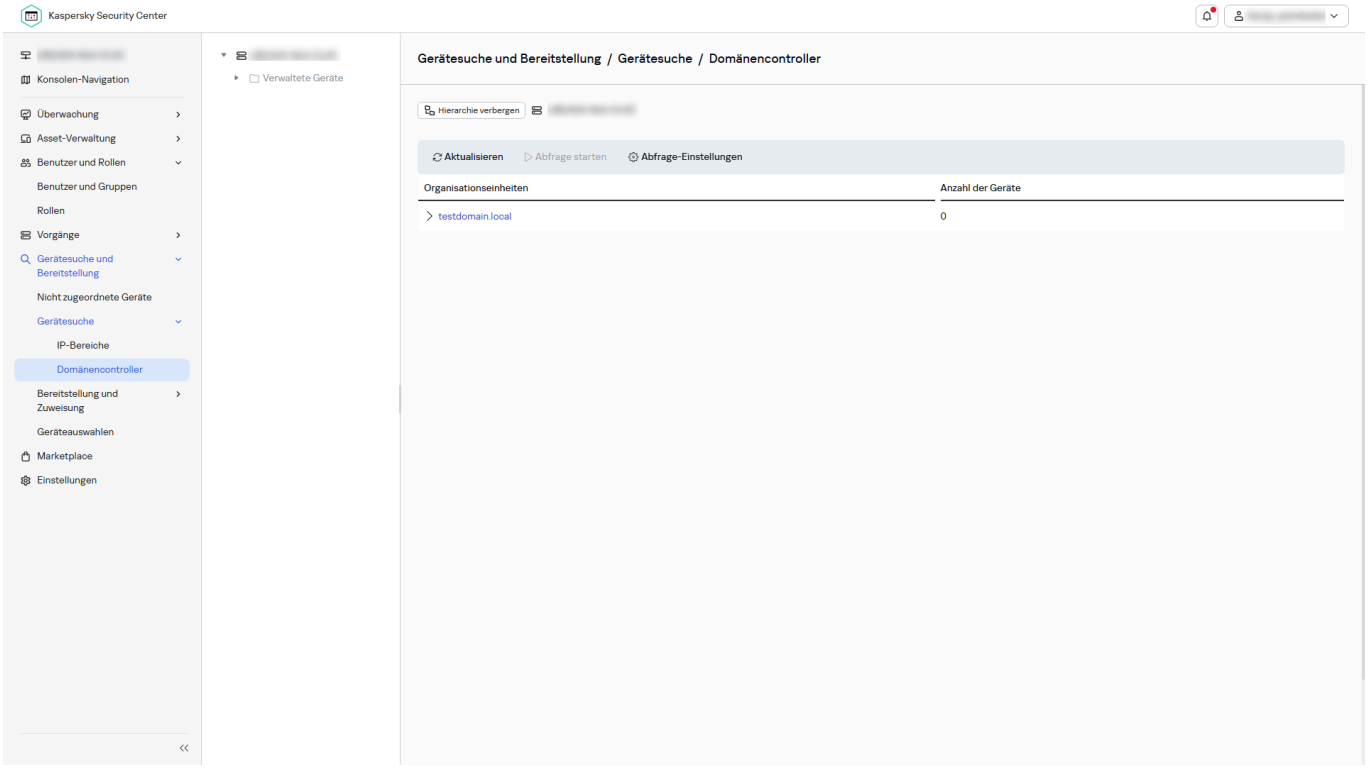
Geben Sie für alle Linux-basierten Hosts innerhalb eines Microsoft Active Directory- oder Samba-Domänencontrollers den `netbios name` und `workgroup`Parameter in der Datei `/etc/samba/smb.conf` an. Andernfalls können Hosts mehrfach in den Abfrageergebnissen enthalten sein.

Wenn eine Domäne von Microsoft Active Directory mehrere Domänencontroller enthält, wird die Auswahl eines bestimmten Controllers während der Domänenabfrage nicht unterstützt. Die Verbindung wird mit dem ersten gefundenen Domänencontroller hergestellt. Um eine ordnungsgemäße Authentifizierung an der Domäne von Microsoft Active Directory sicherzustellen, muss das Feld für den alternativen Antragstellernamen (Subject Alternative Name – SAN) des Zertifikats neben allen Adressen der Domänencontroller, die zu dieser Domäne gehören, auch den NetBIOS-Namen der Domäne von Microsoft Active Directory enthalten.

Abfrage des Domänencontrollers mithilfe des Administrationsservers

So fragen Sie einen Domänencontroller mithilfe des Administrationsservers ab:

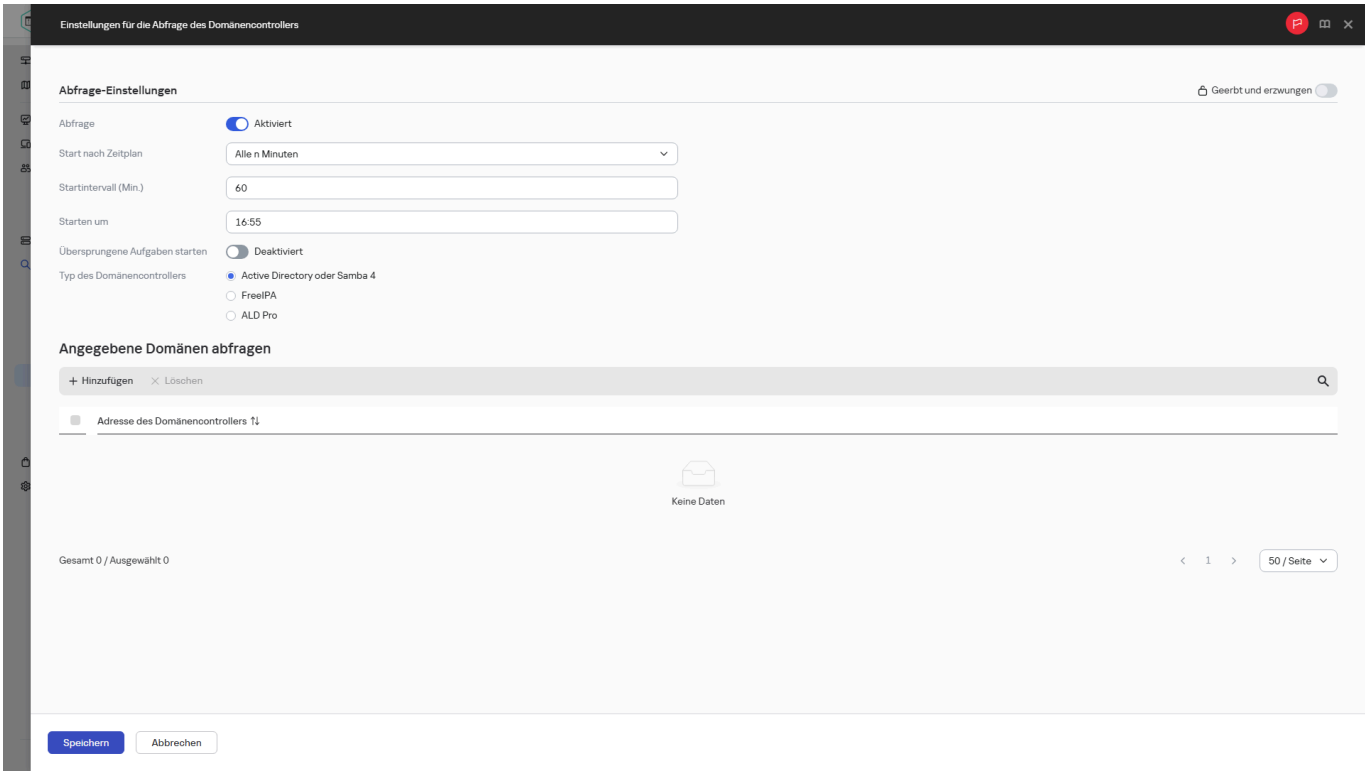
1. Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → Domänencontroller**.



Fenster zur Abfrage des Domänencontrollers

2. Klicken Sie auf **Abfrageeinstellungen anpassen**.

   Das Fenster **Einstellungen für die Abfrage des Domänencontrollers** wird geöffnet.



Einstellungen für die Abfrage des Domänencontrollers

3. Schalten Sie im Feld **Abfrage** den Umschalter in die Position **Aktiviert**.

4. Klicken Sie unter **Angegebene Domänen abfragen** auf **Hinzufügen** und geben Sie anschließend die Adresse und die Anmeldeinformationen des Domänencontrollers an.

5. Gehen Sie im Fenster **Einstellungen für die Abfrage des Domänencontrollers** wie folgt vor:

   - Wählen Sie den Typ des abzufragenden Domänencontrollers aus: **Active Directory oder Samba 4**, **FreeIPA**, **ALD Pro** .

   - Geben Sie erforderlichenfalls den Abfragezeitplan an: Das Standardabfrageintervall beträgt eine Stunde. Die alten Daten werden durch die bei der nächsten Abfrage empfangenen Daten vollständig ersetzt.

     Folgende Varianten sind als Intervall verfügbar:

     - **Alle n Tage**

       Die Abfrage wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Tagen ausgeführt.

       Standardmäßig wird die Abfrage ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

     - **Alle n Minuten**

       Die Abfrage wird ab der angegebenen Uhrzeit regelmäßig im angegebenen Intervall in Minuten ausgeführt.

     - **Nach Wochentagen**

       Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

     - **Monatlich am ausgewählten Tag**

       Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

     - **Übersprungene Aufgaben starten**

       Wenn der Administrationsserver während der für die Abfrage geplanten Zeit abgeschaltet oder nicht verfügbar ist, kann der Administrationsserver die Abfrage entweder sofort nachdem er eingeschaltet wurde starten, oder auf die nächste planmäßige Durchführung warten.

       Wenn diese Option aktiviert ist, startet der Administrationsserver die Abfrage sofort nachdem er eingeschaltet wurde.

       Wenn diese Option deaktiviert ist, wartet der Administrationsserver auf den nächsten Zeitpunkt, für den die Abfrage geplant ist.

       Diese Option ist standardmäßig deaktiviert.

   Wenn Sie Benutzerkonten in einer Sicherheitsgruppe der Domäne ändern, werden diese Änderungen eine Stunde nach Ihrer Abfrage des Domänencontrollers in Kaspersky Security Center Linux angezeigt.

6. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

7. Wenn Sie die Abfrage sofort durchführen möchten, klicken Sie auf die Schaltfläche **Abfrage starten**.

Abfrage des Domänencontrollers mithilfe eines Verteilungspunkts

Sie können einen Domänencontroller auch mithilfe eines Verteilungspunkts abfragen. Als Verteilungspunkt kann ein verwaltetes Windows- oder Linux-Gerät fungieren.

Für einen Linux-Verteilungspunkt wird das Abfragen aller Domänencontroller-Typen unterstützt.
Für einen Windows-Verteilungspunkt wird nur das Abfragen eines Microsoft Active Directory-Domänencontrollers unterstützt.
Das Abfragen mit einem Mac-Verteilungspunkt wird nicht unterstützt.

So konfigurieren Sie die Abfrage von Domänencontrollern mithilfe des Verteilungspunkts:

1. Öffnen Sie die Eigenschaften des Verteilungspunkts.
2. Wählen Sie den Abschnitt **Abfrage des Domänencontrollers** aus.
3. Schalten Sie im Feld **Abfrage** den Umschalter in die Position **Aktiviert**.
4. Wenn Sie einen Linux Verteilungspunkt verwenden, wählen Sie den Typ des abzufragenden Domänencontrollers aus: **Active Directory oder Samba 4**, **FreeIPA**, **ALD Pro**.

   Es ist nicht erforderlich, dass Sie bei der Konfiguration der Abfrage mithilfe eines Verteilungspunkts und mithilfe des Administrationsservers denselben Domänencontroller-Typ angeben.
5. Wählen Sie den Domänencontroller aus, den Sie abfragen möchten.

   Wenn Sie einen Linux-Verteilungspunkt verwenden, klicken Sie im Abschnitt **Angegebene Domänen abfragen** auf **Hinzufügen** und geben Sie anschließend die Adresse und die Anmeldeinformationen des Domänencontrollers an.

   Wenn Sie einen Windows-Verteilungspunkt verwenden, können Sie eine der folgenden Optionen auswählen:

   - **Aktuelle Domäne abfragen**
   - **Domänengesamtstruktur abfragen**
   - **Angegebene Domänen abfragen**
6. Klicken Sie auf die Schaltfläche **Abfragezeitplan festlegen**, um bei Bedarf die Einstellungen des Abfragezeitplans festzulegen.

   Die Abfrage wird nur entsprechend dem festgelegten Zeitplan gestartet. Das manuelle Starten der Abfrage ist nicht möglich.

Nach Abschluss der Abfrage wird die Domänenstruktur im Abschnitt **Domänencontroller** angezeigt.

Wenn Sie Verschiebungsregeln für Geräte eingerichtet und aktiviert haben, werden die kürzlich gefundenen Geräte automatisch in die Gruppe **Verwaltete Geräte** aufgenommen. Wenn keine Verschiebungsregeln aktiviert sind, werden die kürzlich gefundenen Geräte automatisch in die Gruppe **Nicht zugeordnete Geräte** aufgenommen.

Die gefundenen Benutzerkonten können für die Domänenauthentifizierung in Kaspersky Security Center Web Console verwendet werden.

Authentifizierung und Verbindung mit einem Domänencontroller

Authentifizierung und Verbindung mit einem Domänencontroller während einer Domänenabfrage

Während der Abfrage eines Domänencontrollers identifiziert der Administrationsserver oder ein Verteilungspunkt das Verbindungsprotokoll, um die erstmalige Verbindung mit dem Domänencontroller herzustellen. Dieses Protokoll wird für alle zukünftigen Verbindungen zum Domänencontroller verwendet. Wenn Sie die erste Verbindung mit dem Domänencontroller herstellen, können Sie die Verbindungsoptionen mithilfe der Flags des Administrationsagenten (`KLNAG_LDAP_TLS_REQCERT` und `KLNAG_LDAP_SSL_CACERT`) ändern. Die Administrationsagenten-Flags können Sie mithilfe von klscflag konfigurieren, wie in diesem Artikel beschrieben.

Die erstmalige Verbindung mit einem Domänencontroller funktioniert wie folgt:

1. Der Administrationsserver oder ein Verteilungspunkt versucht, über LDAPS eine Verbindung mit dem Domänencontroller herzustellen.

   Standardmäßig ist keine Überprüfung des Zertifikats notwendig. Um die Überprüfung des Zertifikats zu erzwingen, setzen Sie das Flag `KLNAG_LDAP_TLS_REQCERT` auf "1".

   Mögliche Einstellungswerte des Parameters `KLNAG_LDAP_TLS_REQCERT`:

   - `0` – Das Zertifikat wird angefordert, aber wenn es nicht bereitgestellt wurde oder die Überprüfung des Zertifikats fehlgeschlagen ist, gilt die TLS-Verbindung dennoch als erfolgreich hergestellt (Standardwert).
   - `1` – Eine strenge Überprüfung des LDAP-Serverzertifikats ist erforderlich.

   Wenn das Flag `KLNAG_LDAP_SSL_CACERT` nicht angegeben ist, wird standardmäßig für den Zugriff auf die Zertifikatskette der vom Betriebssystem abhängige Pfad zur Zertifizierungsstelle (CA) verwendet. Um einen benutzerdefinierten Pfad anzugeben, verwenden Sie das Flag `KLNAG_LDAP_SSL_CACERT`.

2. Wenn die LDAPS-Verbindung fehlschlägt, versucht der Administrationsserver oder ein Verteilungspunkt, über eine unverschlüsselte TCP-Verbindung unter Verwendung von SASL (DIGEST-MD5) eine Verbindung zum Domänencontroller herzustellen.

Authentifizierung und Verbindung mit einem Domänencontroller während der Authentifizierung eines Domänenbenutzers auf dem Administrationsserver

Wenn sich ein Domänenbenutzer auf dem Administrationsserver authentifiziert, identifiziert der Administrationsserver das Protokoll für den Verbindungsaufbau zum Domänencontroller.

Für FreeIPA und ALD Pro werden die LDAP- und LDAPS-Protokolle nur für die Domänenabfrage verwendet. Kaspersky Security Center Linux unterstützt die Authentifizierung von FreeIPA-Benutzerkonten über LDAP bzw. LDAPS nicht. Damit sich FreeIPA- und ALD Pro-Benutzer an der Web Console anmelden können, müssen Sie die Kerberos-Authentifizierung über den IAM-Dienst konfigurieren.

Die Verbindung mit einem Domänencontroller funktioniert wie folgt:

1. Der Administrationsserver versucht, über LDAPS eine Verbindung zum Domänencontroller herzustellen.

   Es ist eine strenge Überprüfung des LDAP-Serverzertifikats erforderlich.

   Wenn das Flag `KLNAG_LDAP_SSL_CACERT` nicht angegeben ist, wird standardmäßig für den Zugriff auf die Zertifikatskette der vom Betriebssystem abhängige Pfad zur Zertifizierungsstelle (CA) verwendet. Um einen benutzerdefinierten Pfad anzugeben, verwenden Sie das Flag `KLNAG_LDAP_SSL_CACERT`.

2. Wenn die LDAPS-Verbindung fehlschlägt, tritt ein Verbindungsfehler für den Domänencontroller auf und es werden keine anderen Verbindungsprotokolle verwendet.

Flags konfigurieren

Sie können die Parameter mithilfe des Tools "klscflag" konfigurieren.

Öffnen Sie die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Auf dem Gerät mit dem Administrationsserver befindet sich das Dienstprogramm "klscflag" im Installationsverzeichnis. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

Der folgende Befehl erzwingt beispielsweise die Überprüfung des Zertifikats:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Einen Samba-Domänencontroller konfigurieren

Kaspersky Security Center Linux unterstützt einen Linux-Domänencontroller, der nur auf Samba 4 ausgeführt wird.

Ein Samba-Domänencontroller unterstützt die gleichen Schema-Erweiterungen wie ein Domänencontroller von Microsoft Active Directory. Sie können die vollständige Kompatibilität eines Samba-Domänencontrollers mit einem Microsoft Active Directory-Domänencontroller aktivieren, indem Sie die Samba 4-Schema-Erweiterung verwenden. Dies ist eine optionale Aktion.

> Es wird empfohlen, die vollständige Kompatibilität eines Samba-Domänencontrollers mit einem Microsoft Active Directory-Domänencontroller zu aktivieren. Dadurch wird die korrekte Interaktion zwischen Kaspersky Security Center Linux und dem Samba-Domänencontroller gewährleistet.

So aktivieren Sie die vollständige Kompatibilität eines Samba-Domänencontrollers mit einem Microsoft Active Directory-Domänencontroller:

1. Führen Sie den folgenden Befehl aus, um die Schema-Erweiterung "RFC2307" zu verwenden:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Aktivieren Sie auf einem Samba-Domänencontroller das Schema-Update. Fügen Sie dafür der Datei `/etc/samba/smb.conf` die folgende Zeile hinzu:

   ```
   dsdb:schema update allowed = true
   ```

   > Wenn das Schema-Update mit einem Fehler abgeschlossen wird, müssen Sie eine vollständige Wiederherstellung jenes Domänencontrollers durchführen, der als Schema-Master agiert.

Geben Sie für alle Linux-basierten Hosts innerhalb eines Samba-Domänencontrollers die Parameter `netbios name` und `workgroup` in der Datei `/etc/samba/smb.conf` an. Andernfalls können Hosts mehrfach in den Abfrageergebnissen enthalten sein.

Hardware-Inventur

Die Hardware-Liste (**Asset-Verwaltung** → **Hardware**), die Sie für die Inventur der Hardware verwenden, wird auf zwei Arten gefüllt: automatisch und manuell. Nach jeder Netzwerkabfrage werden alle erkannten Geräte automatisch in die Liste eingetragen. Sie können Geräte aber auch manuell hinzufügen, wenn Sie das Netzwerk nicht abfragen möchten. Sie können manuell weitere Geräte zu der Liste hinzufügen, z. B. Router, Drucker und andere Geräte-Hardware.

In den Eigenschaften eines Geräts können Sie sich ausführliche Informationen über das Gerät anzeigen lassen und diese bearbeiten.

Die Hardware-Liste kann die folgenden Gerätetypen enthalten:

- Computer
- Mobile Geräte
- Netzwerkgeräte
- virtuelle Geräte
- Computer-Hardware (OEM)
- Computer-Peripheriegeräte
- angeschlossene Geräte
- VoIP-Telefonie
- Netzwerkspeicher

Der Administrator kann den gefundenen Geräten das Merkmal *Für Unternehmen* zuweisen. Er kann dieses Merkmal in den Eigenschaften des Geräts manuell zuweisen oder die Kriterien für die automatische Zuweisung festlegen. In diesem Fall wird das Merkmal *Für Unternehmen* nach dem Typ des Geräts zugewiesen.

Kaspersky Security Center Linux ermöglicht die Abschreibung von Hardware. Aktivieren Sie dazu in den Eigenschaften des Geräts die Option **Abgeschrieben**. Ein solches Gerät wird in der Hardware-Liste nicht angezeigt.

Der Administrator kann im Ordner **Hardware** die Liste der speicherprogrammierbaren Steuerungen (SPS) verwenden. Ausführliche Informationen zur Verwendung von SPS-Listen finden Sie im *Benutzerhandbuch für Kaspersky Industrial CyberSecurity for Nodes*.

Informationen über neue Geräte hinzufügen

Um Informationen über neue Geräte hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Hardware**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**, um das Fenster **Neues Gerät** zu öffnen.
3. Wählen Sie im Fenster **Neues Gerät** in der Dropdown-Liste **Gerätetyp** den Typ des Gerätes aus, das Sie hinzufügen möchten.
4. Klicken Sie auf die Schaltfläche **OK**.

   Das Fenster mit den Geräte-Eigenschaften im Abschnitt **Allgemein** wird geöffnet.
5. Füllen Sie im Abschnitt **Allgemein** die Eingabefelder mit den Daten über das Gerät aus. Im Abschnitt **Allgemein** werden die folgenden Einstellungen angezeigt:

   - **Unternehmensgerät**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie dem Gerät das Merkmal *Für Unternehmen* zuweisen möchten. Nach diesem Merkmal können Sie Suche nach Geräten im Ordner **Hardware** durchführen.
   - **Abgeschrieben**. Aktivieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass das Gerät in der Geräteliste im Ordner **Hardware** angezeigt wird.
6. Klicken Sie auf die Schaltfläche **Übernehmen**.

Das neue Gerät wird im Arbeitsbereich auf der Seite **Hardware** angezeigt.

Kriterien zur Erkennung von Unternehmensgeräten anpassen

Um Kriterien zur Erkennung von Unternehmensgeräten anzupassen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Hardware**.
2. Klicken Sie im oberen Bereich der Seite **Hardware** auf den Link **Regel für Geräte mit Merkmal "Unternehmensgerät" einrichten**.

   Der Bereich **Regel für Geräte mit Merkmal "Unternehmensgerät" einrichten** wird aufgerufen.
3. Aktivieren Sie im Bereich **Regel für Geräte mit Merkmal "Unternehmensgerät" einrichten** die Option **Merkmal "Unternehmensgerät" für das Gerät automatisch setzen**. Geben Sie Gerätetypen an, denen das Attribut *Enterprise* automatisch zugewiesen wird.

   > Diese Option wirkt sich nur auf die Geräte aus, die durch Netzwerkabfrage hinzugefügt wurden. Stellen Sie für die manuell hinzugefügten Geräte das Merkmal *Für Unternehmen* manuell ein.
4. Klicken Sie auf die Schaltfläche **OK**.

Die Kriterien zur Bestimmung von Unternehmensgeräte sind konfiguriert.

Dynamischen VDI-Modus auf Client-Geräten verwenden

Im Netzwerk eines Unternehmens kann eine virtuelle Infrastruktur mittels temporärer Nutzung virtueller Maschinen bereitgestellt werden. Kaspersky Security Center Linux erkennt temporäre virtuelle Maschinen und fügt ihre Daten zur Administrationsserver-Datenbank hinzu. Nachdem der Benutzer seine Arbeit auf der temporären virtuellen Maschine beendet hat, wird die virtuelle Maschine aus der virtuellen Infrastruktur entfernt. Der Eintrag der virtuellen Maschine kann jedoch in der Administrationsserver-Datenbank gespeichert werden. Zudem können nicht vorhandene virtuelle Maschinen in der Kaspersky Security Center Web Console angezeigt werden.

Damit keine Daten über nicht vorhandene virtuelle Maschinen gespeichert werden, wurde in Kaspersky Security Center Linux die Unterstützung des dynamischen Modus für die Virtual Desktop Infrastructure (VDI) realisiert. Der Administrator kann die Unterstützung des dynamischen Modus für VDI in den Eigenschaften des Installationspakets des Administrationsagenten aktivieren, das auf einer temporären virtuellen Maschine installiert wird.

Wird die temporäre virtuelle Maschine heruntergefahren, informiert der Administrationsagent darüber den Administrationsserver. Wurde die virtuelle Maschine erfolgreich heruntergefahren, wird sie aus der Liste der Geräte entfernt, die mit dem Administrationsserver verbunden sind. Wurde die virtuelle Maschine fehlerhaft heruntergefahren, und der Administrationsagent hat keine Benachrichtigung darüber an den Administrationsserver gesendet, wird eine Backup-Szenario angewendet. In diesem Fall wird die virtuelle Maschine nach drei fehlgeschlagenen Synchronisierungsversuchen mit dem Server aus der Liste der mit dem Administrationsserver verbundenen Geräte entfernt.

Dynamischen VDI-Modus in den Eigenschaften des Installationspakets des Administrationsagenten aktivieren

Gehen Sie wie folgt vor, um den dynamischen VDI-Modus zu aktivieren:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung** → **Installationspakete**.
2. Klicken Sie mit der rechten Maustaste auf das Installationspaket des Administrationsagenten und wählen Sie **Eigenschaften** aus.

   Daraufhin wird das Fenster **Eigenschaften** geöffnet.
3. Wählen Sie im Fenster **Eigenschaften** den Abschnitt **Erweitert** aus.
4. Aktivieren Sie auf der Registerkarte **Erweitert** die Option **Dynamischen Modus für VDI aktivieren**.

Das Gerät mit dem zu installierenden Administrationsagenten wird ein Teil der VDI.

Geräte, die zu VDI gehören, in eine Administrationsgruppe verschieben

Gehen Sie wie folgt vor, um Geräte, die zur VDI gehören, in eine Administrationsgruppe zu verschieben:

1. Gehen Sie zu **Asset-Verwaltung** → **Verschiebungsregeln**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Wählen Sie auf der Registerkarte **Regelbedingungen** die Registerkarte **Virtuelle Maschinen** aus.
4. Setzen Sie die Regel **Ist eine virtuelle Maschine** auf **Ja** und **Gehört zur Virtual Desktop Infrastructure (VDI)** auf **Ja**.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Client-Geräte verwalten

Mit Kaspersky Security Center Linux können Sie Client-Geräte verwalten:

- Einstellungen und Status von verwalteten Geräten anzeigen, einschließlich Clustern und Server-Arrays.
- Verteilungspunkte konfigurieren.
- Aufgaben verwalten.

Sie können Administrationsgruppen verwenden, um Client-Geräte zu einem Satz zusammenzufassen, der als eine einzige Einheit verwaltet werden kann. Ein Client-Gerät kann nur in einer Administrationsgruppe enthalten sein. Geräte können auf der Grundlage von **Regelbedingungen** automatisch einer Gruppe zugewiesen werden:

- Regeln für das Verschieben von Geräten erstellen.
- Regeln für das Verschieben von Geräten kopieren.
- Bedingungen für eine Verschiebungsregel für Geräte.

Sie können Geräteauswahlen verwenden, um Geräte basierend auf einer Bedingung zu filtern. Sie können auch Geräte markieren, um eine Auswahl zu erstellen, Geräte zu finden und Geräte auf Administrationsgruppen zu verteilen.

Einstellungen eines verwalteten Geräts

So zeigen Sie die Einstellungen eines verwalteten Geräts an:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte)**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des entsprechenden Geräts.

Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.

Im oberen Bereich des Eigenschaftenfensters werden die folgenden Registerkarten mit den wichtigsten Einstellungsgruppen angezeigt:

- **Allgemein**

  Diese Registerkarte umfasst die folgenden Abschnitte:

  - Der Abschnitt **Allgemein** enthält allgemeine Informationen über das Client-Gerät. Die Informationen beruhen auf Daten, die bei der letzten Synchronisierung des Client-Geräts mit dem Administrationsserver empfangen wurden:

    - **Name**

      In diesem Feld steht der Name des Client-Geräts in der Administrationsgruppe und der Name kann geändert werden.

- **Beschreibung**

  In diesem Feld können Sie eine zusätzliche Beschreibung für das Client-Gerät eingeben.

- **Gerätestatus**

  Status des Client-Geräts. Dieser Status beruht auf den Kriterien, die der Administrator für den Status des Antiviren-Schutzes und die Aktivität des Geräts im Netzwerk festlegt.

- **Gerätebesitzer**

  Name des Gerätebesitzers. Sie können einen Benutzer als Gerätebesitzer zuweisen oder entfernen. Dazu dient der Link **Gerätebesitzer verwalten**.

- **Vollständiger Gruppenname**

  Administrationsgruppe, zu der das Client-Gerät gehört.

- **Letzte Aktualisierung der Antiviren-Datenbanken**

  Datum des letzten Updates der Antiviren-Datenbanken oder der Anwendungen auf dem Gerät.

- **Verbindung mit dem Administrationsserver**

  Datum und Uhrzeit der letzten Verbindung des auf dem Client-Gerät installierten Administrationsagenten mit dem Administrationsserver.

- **Zuletzt im Netzwerk sichtbar**

  Zeitpunkt (Datum und Uhrzeit), zu dem das Gerät zuletzt im Netzwerk gesehen wurde.

- **Version des Administrationsagenten**

  Version des installierten Administrationsagenten.

- **Erstellt**

  Datum, an dem das Gerät innerhalb von Kaspersky Security Center Linux erstellt wurde.

- **Verbindung mit Administrationsserver nicht trennen**

  Wenn diese Option aktiviert ist, wird die dauerhafte Verbindung zwischen dem verwalteten Gerät und dem Administrationsserver aufrecht erhalten. Sie können diese Option verwenden, wenn Sie keine Push-Server einsetzen, die eine solche Verbindung bereitstellen.

  Wenn diese Option deaktiviert ist und keine Push-Server verwendet werden, verbindet sich das verwaltete Gerät nur zur Datensynchronisierung oder Datenübertragung mit dem Administrationsserver.

  Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

  Diese Option ist auf verwalteten Geräten standardmäßig deaktiviert. Diese Option ist auf dem Gerät, auf dem der Administrationsserver installiert ist, standardmäßig aktiviert und bleibt selbst dann aktiviert, wenn Sie versuchen, sie zu deaktivieren.

- **Sitzungen**

  Dieser Abschnitt enthält eine Tabelle mit Informationen zu den Benutzern, die aktuell am Gerät angemeldet sind. Die Tabelle zeigt die folgende Daten in den entsprechenden Spalten an:

  - Benutzername
  - Name des SAM-Kontos
  - Benutzer-Principal-Name (UPN)
  - E-Mail-Adresse

  Um Informationen über die Sitzungen von Domänenbenutzern korrekt anzuzeigen, müssen Sie die Abfrage des Domänencontrollers verwenden.

- Der Abschnitt **Netzwerk** enthält folgende Informationen zu den Netzwerkeinstellungen des Client-Geräts:

  - **IP-Adresse**

    IP-Adresse des Geräts.

  - **Windows-Domäne**

    Arbeitsgruppe, in der das Gerät enthalten ist.

  - **DNS-Name**

    Name der DNS-Domäne des Client-Geräts.

  - **NetBIOS-Name**

    Name des Client-Geräts.

  - **IPv6-Adresse**

- Der Abschnitt **System** enthält Daten zum Betriebssystem, das auf dem Client-Gerät installiert ist:

  - **Betriebssystem**
  - **CPU-Architektur**
  - **Gerätename**
  - **Typ der virtuellen Maschine**

    Hersteller der virtuellen Maschine.

  - **Dynamische virtuelle Maschine als Teil von VDI**

    Diese Zeile gibt an, ob das Client-Gerät eine dynamische virtuelle Maschine als Teil einer VDI ist.

- Der Abschnitt **Schutz** enthält folgende Informationen über den Status des Antiviren-Schutzes auf dem Client-Gerät:

  - **Sichtbar**

    Sichtbarkeitsstatus des Client-Geräts.

- **Gerätestatus**

  Status des Client-Geräts, der ihm anhand der vom Administrator festgelegten Kriterien den Status des Antiviren-Schutzes und der Aktivität des Geräts im Netzwerk zugewiesen wird.

- **Statusbeschreibung**

  Status des Schutzes für das Client-Gerät und der Verbindung zum Administrationsserver.

- **Schutzstatus**

  Dieses Feld enthält den aktuellen Status des Echtzeitschutzes auf dem Client-Gerät.

  Wenn sich der Status auf dem Gerät ändert, wird der neue Status erst im Eigenschaftenfenster des Geräts angezeigt, nachdem das Client-Gerät mit dem Administrationsserver synchronisiert wurde.

- **Letzte vollständige Untersuchung**

  Datum und Uhrzeit der letzten Schadsoftware-Untersuchung auf einem Client-Gerät.

- **Virus gefunden**

  Gesamtzahl der auf dem Client-Gerät gefundenen Bedrohungen seit der Installation der Sicherheitsanwendung (seit der ersten Untersuchung des Geräts) oder seit dem letzten Zurücksetzen des Zählers.

- **Objekte, die nicht desinfiziert werden konnten**

  Anzahl der unverarbeiteten Dateien auf einem Client-Gerät.

  In diesem Feld wird die Anzahl der unverarbeiteten Dateien auf mobilen Geräten nicht berücksichtigt.

- **Status der Datenträgerverschlüsselung**

  Aktueller Status der Verschlüsselung von Dateien auf den lokalen Laufwerken des Geräts. Eine Beschreibung der Statuswerte finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

  Dateien können nur auf den verwalteten Geräten verschlüsselt werden, auf denen Kaspersky Endpoint Security für Windows installiert ist.

- Der Abschnitt **Gerätestatus wird durch Anwendung bestimmt** enthält Daten über den Gerätestatus, der durch die auf dem Gerät installierte, verwaltete Anwendung bestimmt wird. Der Gerätestatus kann vom durch Kaspersky Security Center Linux zugewiesenen Status abweichen.

- **Anwendungen**

  Diese Registerkarte listet alle Kaspersky-Anwendungen auf, die auf dem Client-Gerät installiert sind. Auf dieser Registerkarte befinden sich die Schaltflächen **Starten** und **Stoppen**, mit denen Sie erforderliche Kaspersky-Anwendungen (mit Ausnahme des Administrationsagenten) starten und stoppen können. Sie können diese Schaltflächen verwenden, wenn auf dem verwalteten Gerät der UDP-Port 15000 für den Empfang von Push-Benachrichtigungen vom Administrationsserver verfügbar ist. Wenn das verwaltete Gerät nicht für Push-Benachrichtigungen verfügbar ist, aber der Modus für die dauerhafte Verbindung mit dem Administrationsserver aktiviert ist (d. h., im Abschnitt **Allgemein** ist die Option **Verbindung mit Administrationsserver nicht trennen** aktiviert), stehen die Schaltflächen **Starten** und **Stoppen** auch zur Verfügung. Andernfalls wird beim Versuch, die Anwendung zu starten oder zu stoppen, eine Fehlermeldung ausgegeben. Sie können auch auf die Namen der Anwendungen klicken, um sich allgemeine Informationen über eine Anwendung, eine Liste mit allen auf dem Gerät aufgetretenen Ereignissen und die Einstellungen der Anwendung anzeigen zu lassen.

- **Aktive Richtlinien und Richtlinienprofile**

  Diese Registerkarte listet die Richtlinien und Richtlinienprofile auf, die dem verwalteten Gerät derzeit zugewiesen sind.

- **Aufgaben**

  Auf der Registerkarte **Aufgaben** können Sie die Aufgaben eines Client-Geräts verwalten: Liste der vorhandenen Aufgaben anzeigen, neue Aufgaben erstellen, Aufgaben entfernen, starten und beenden, Aufgabeneinstellungen ändern und die Ergebnisse der Aufgabenausführung anzeigen. Die Aufgabenliste beruht auf Daten, die während der letzten Synchronisierung des Clients mit dem Administrationsserver empfangen wurden. Die Daten über den Aufgabenstatus erhält der Administrationsserver vom Client-Gerät. Wenn auf dem verwalteten Gerät der UDP-Port 15000 für den Empfang von Push-Benachrichtigungen vom Administrationsserver verfügbar ist, werden der Aufgabenstatus angezeigt und die Schaltflächen zur Aufgabenverwaltung aktiviert. Wenn der Push-Server das verwaltete Gerät nicht erreichen kann, aber der Modus für die dauerhafte Verbindung mit dem Administrationsserver aktiviert ist (d. h., im Abschnitt **Allgemein** ist die Option **Verbindung mit Administrationsserver nicht trennen** aktiviert), stehen die Aktionen für die Aufgaben auch zur Verfügung.

  Wenn keine Verbindung besteht, wird kein Status angezeigt und die Schaltflächen sind nicht verfügbar.

- **Ereignisse**

  Die Registerkarte **Ereignisse** enthält die Ereignisse, die für das ausgewählte Client-Gerät auf dem Administrationsserver registriert wurden.

  Sie können die Ereignisse von Geräten exportieren, kopieren und löschen.

- **Sicherheitsprobleme**

  Auf der Registerkarte **Sicherheitsprobleme** können Sie Sicherheitsvorfälle für ein Client-Gerät anzeigen, bearbeiten oder erstellen. Sicherheitsvorfälle können sowohl automatisch mithilfe von auf dem Client-Gerät installierten verwalteten Kaspersky-Anwendungen als auch manuell vom Administrator erstellt werden. Wenn beispielsweise einige Benutzer immer wieder Schadsoftware von Wechseldatenträgern auf Geräte übertragen, kann der Administrator einen Sicherheitsvorfall erstellen. Der Administrator kann im Text des Sicherheitsvorfalls eine kurze Beschreibung des Falls bereitstellen und Aktionen vorschlagen (etwa Disziplinarmaßnahmen gegen einen Benutzer) und einen Link zum Benutzer oder zu den Benutzern hinzufügen.

  Ein Vorfall, für den alle erforderlichen Aktionen ausgeführt worden sind, wird als *Bearbeitet* bezeichnet. Das Vorhandensein von nicht bearbeiteten Sicherheitsvorfällen kann als Bedingung für eine Statusänderung des Geräts in *Kritisch* oder *Warnung* ausgewählt werden.

  Dieser Abschnitt enthält eine Liste der für das Gerät erstellten Sicherheitsvorfälle. Die Sicherheitsvorfälle werden nach Signifikanz und Art eingestuft. Die Art des Sicherheitsvorfalls wird von der Kaspersky-Anwendung bestimmt, die den Vorfall erstellt hat. Bearbeitete Sicherheitsvorfälle können in der Liste durch Aktivieren des Kontrollkästchens in der Spalte **Bearbeitet** gekennzeichnet werden.

- **Tags**

  Auf der Registerkarte **Tags** können Sie die Liste der Schlüsselwörter verwalten, auf deren Grundlage die Suche nach Client-Geräten ausgeführt wird: Liste der vorhandenen Tags anzeigen, Tags aus der Liste zuweisen, Regeln für die automatische Zuweisung von Tags konfigurieren, neue Tags hinzufügen und alte Tags umbenennen sowie Tags löschen.

- **Erweitert**

  Diese Registerkarte umfasst die folgenden Abschnitte:

  - **Programm-Registry**. In diesem Abschnitt können Sie die Registry der auf dem Client-Gerät installierten Anwendungen und der Anwendungs-Updates anzeigen lassen und die Darstellung der Programm-Registry konfigurieren.

    Informationen über die installierten Anwendungen sind verfügbar, wenn der auf dem Client-Gerät installierte Administrationsagent die erforderlichen Daten an den Administrationsserver überträgt. Die Einstellungen für die Übertragung der Informationen an den Administrationsserver können Sie im Eigenschaftenfenster des Administrationsagenten oder seiner Richtlinie im Abschnitt **Datenverwaltung** anpassen.

    Durch Klicken auf einen Anwendungsnamen wird ein Fenster geöffnet, das die Anwendungsdetails und eine Liste der für die Anwendung installierten Update-Pakete enthält.

  - **Ausführbare Dateien**. Dieser Abschnitt enthält ausführbare Dateien, die auf dem Client-Gerät gefunden wurden.

  - **Verteilungspunkte**. Dieser Abschnitt enthält eine Liste der Verteilungspunkte, mit denen das Gerät interagiert.

    - **In Datei exportieren**

      Mithilfe der Schaltfläche **In Datei exportieren** können Sie die Liste der Verteilungspunkte, mit denen das Gerät interagiert, in einer Datei speichern. Standardmäßig exportiert die Anwendung die Liste der Geräte in eine Datei im csv-Format.

    - **Eigenschaften**

      Mithilfe der Schaltfläche **Eigenschaften** können Sie die Einstellungen der Verteilungspunkte, mit denen das Gerät interagiert, anzeigen und anpassen.

  - **Hardware-Register**. Dieser Abschnitt enthält Informationen zur Hardware, die auf dem Client-Gerät installiert ist.

    Wenn der Administrationsagent auf einem Windows-Gerät installiert ist, sendet er nur die folgenden Informationen über die Gerätehardware an den Administrationsserver:

    - Arbeitsspeicher
    - Massenspeichergeräte
    - Mainboard
    - Prozessor
    - Netzwerkadapter
    - Monitore
    - Grafikkarte
    - Soundkarte

Wenn der Administrationsagent auf einem Linux- oder macOS-Gerät installiert ist, sendet er die folgenden Informationen über die Gerätehardware an den Administrationsserver (vorausgesetzt, diese Information wird durch das Betriebssystem bereitgestellt):

- Gesamtgröße des Arbeitsspeichers
- Gesamtgröße der Massenspeicher
- Mainboard
- Prozessor
- Netzwerkadapter

- **Verfügbare Updates**. Dieser Abschnitt enthält eine Liste der auf dem Gerät gefundenen Programm-Updates, die noch nicht installiert wurden.

- **Schwachstellen in Programmen**. Dieser Abschnitt bietet Informationen über die Schwachstellen von Drittanbieter-Anwendung, die auf den Client-Geräten installiert sind.

  Um die Schwachstellen in einer Datei zu speichern, aktivieren Sie die Kontrollkästchen neben den betreffenden Schwachstellen und klicken Sie dann auf die Schaltfläche **In csv-Datei exportieren** oder **In txt-Datei exportieren**.

  Dieser Abschnitt enthält die folgenden Einstellungen:

  - **Nur Schwachstellen anzeigen, die geschlossen werden können**

    Ist diese Option aktiviert, werden in diesem Abschnitt jene Schwachstellen angezeigt, die durch einen Patch geschlossen werden können.

    Ist diese Option deaktiviert, werden in diesem Abschnitt sowohl Schwachstellen angezeigt, die durch einen Patch geschlossen werden können, als auch Schwachstellen, für die kein Patch vorhanden ist.

    Diese Option ist standardmäßig aktiviert.

  - **Schwachstellen-Eigenschaften**

    Wählen Sie in der Liste eine Software-Schwachstelle aus, um die Eigenschaften der ausgewählten Software-Schwachstelle in einem separaten Fenster anzuzeigen. In dem Fenster können Sie Folgendes tun:

    - Schwachstellen in Programmen auf diesem verwalteten Gerät ignorieren (in der Kaspersky Security Center Web Console).
    - Liste mit Korrekturen anzeigen, die für die Schwachstelle empfohlen werden.
    - Programm-Updates manuell angeben, um eine Schwachstelle zu beheben (in der Kaspersky Security Center Web Console).
    - Schwachstellen-Instanzen anzeigen.
    - Liste der vorhandenen Aufgaben zur Schwachstellen-Behebung anzeigen und neue Aufgaben zur Schwachstellen-Behebung erstellen.

- **Remote-Diagnose**. In diesem Abschnitt können Sie die Ferndiagnose von Client-Geräten durchführen.

Wenn Sie PostgreSQL, MariaDB oder MySQL als DBMS verwenden, wird auf der Registerkarte **Ereignisse** möglicherweise eine unvollständige Liste der Ereignisse für das ausgewählte Client-Gerät angezeigt. Dies kommt vor, wenn das DBMS eine sehr große Anzahl von Ereignissen speichert. Sie können die Anzahl der angezeigten Ereignisse auf eine der folgenden Arten erhöhen:

- Nicht benötigte Ereignisse entfernen.
- Speicherdauer für nicht benötigte Ereignisse verkürzen.

Verwenden Sie die Berichte, um eine vollständige Liste der auf dem Administrationsserver für das Gerät protokollierten Ereignisse anzuzeigen.

Verbindung des Client-Geräts mit dem Administrationsserver manuell prüfen. Tool klnagchk

Sie können die Verbindung zwischen einem Client-Gerät und dem Administrationsserver mit dem Tool "klnagchk" überprüfen. Darüber hinaus können Sie mit dem Tool ausführliche Informationen über die Verbindungseinstellungen zwischen dem Client-Gerät und dem Administrationsserver erhalten. Das Tool "klnagchk" befindet sich im Installationsordner des Administrationsagenten.

Beim Starten über die Befehlszeile führt das Tool "klnagchk" je nach Parameter die folgenden Aktionen aus:

- Es zeigt eine Meldung auf dem Bildschirm an oder nimmt eine Eintragung in der Log-Datei der Einstellungswerte für die Verbindung vor, die zwischen dem Administrationsagenten des Geräts und dem Administrationsserver besteht.
- Es trägt in einer Ereignisprotokolldatei die Statistik des Administrationsagenten (beginnend mit dessen letztem Start) und die Ausführungsergebnisse des Tools ein, oder es gibt diese Informationen auf dem Bildschirm aus.
- Es versucht eine Verbindung zwischen dem Administrationsagenten und Administrationsserver herzustellen.

  Bei fehlgeschlagenem Verbindungsaufbau sendet das Tool ein ICMP-Paket an das Gerät, um den Status des Geräts zu überprüfen, auf dem der Administrationsserver installiert ist.

So prüfen Sie die Verbindung zwischen einem Client-Gerät und dem Administrationsserver mit dem Tool "klnagchk":

Starten Sie auf dem Gerät mit installiertem Administrationsagenten das Tool "klnagchk" über die Befehlszeile und unter Verwendung eines lokalen Administratorkontos.

Die Befehlszeilensyntax des Tools lautet:

```
klnagchk [-logfile <Dateiname>] [-sp] [-savecert <Pfad zur Zertifikatsdatei>] [-
restart][-sendhb]
```

Beschreibung der Parameter:

- `-logfile <Dateiname>` – Schreibt die Parameterwerte für die Verbindung zwischen Administrationsagenten und Administrationsserver sowie die Ausführungsergebnisse des Tools in eine Protokolldatei.

  Standardmäßig werden diese Informationen im Standardausgabe-Stream (stdout) gespeichert. Wenn das Argument nicht verwendet wird, werden die Einstellungen, Ergebnisse und Fehlermeldungen auf dem Bildschirm ausgegeben.

- `-sp` – Zeigt bei der Ausgabe das Kennwort für Authentifizierung des Benutzers am Proxy-Server.

  Dieses Argument wird verwendet, wenn die Verbindung zum Administrationsserver über einen Proxy-Server aufgebaut wird.

- `-savecert <Dateiname>` – Speichert das Zertifikat für den Zugriff auf den Administrationsserver in der angegebenen Datei.

- `-restart` – Startet den Administrationsagenten nach Abschluss des Tools.

- `-sendhb` – Startet die Synchronisation des Administrationsagenten mit dem Administrationsserver.

Nach dem Start greift das Tool "klnagchk" auf die Konfigurationsdateien des Administrationsagenten zu und zeigt die Verbindungsparameter an. Die folgenden Parameter werden während der Installation des Administrationsagenten und in den Richtlinieneinstellungen des Administrationsagenten angegeben:

- `Current device` – Name des Client-Geräts im Windows-Netzwerk

- `Network Agent version` – Vollständige Versionsnummer des auf dem Gerät installierten Administrationsagenten (mit Patches)

- `Administration Server address` – Adresse des Administrationsservers

- `Use SSL` – Parameter zur Angabe, ob die Verbindung mit dem Administrationsserver gesichert ist

  Mögliche Werte:

  - 0 – Es wird keine sichere Verbindung verwendet.

  - 1 – Es wird eine sichere Verbindung verwendet.

- `Compress traffic` – Parameter zur Angabe, ob der Datenverkehr zwischen dem Client-Gerät und dem Administrationsserver komprimiert wird

- `Numbers of the Administration Server SSL ports` – Nummern der gültigen Ports für die Kommunikation mit dem Administrationsserver, wenn eine sichere Verbindung verwendet wird.

- `Numbers of the Administration Server ports` – Anzahl der gültigen Ports für die Kommunikation mit dem Administrationsserver, wenn eine normale Verbindung verwendet wird.

- `Use proxy server` – Parameter zur Angabe, ob ein Proxyserver verwendet wird

  Mögliche Werte:

  - 0 – Es wird kein Proxyserver verwendet.

  - 1 – Es wird ein Proxyserver verwendet.

- `Address` – Adresse und Port des Proxyservers, getrennt durch einen Doppelpunkt. Dieser Parameter wird nur angezeigt, wenn ein Proxyserver verwendet wird.

- `User name` – Benutzername für den Zugriff auf den Proxyserver. Dieser Parameter wird nur angezeigt, wenn ein Proxyserver verwendet wird.

- `Password` – Kennwort für den Zugriff auf den Proxyserver. Dieser Parameter wird nur angezeigt, wenn ein Proxyserver verwendet wird. Um das Kennwort des Proxyservers anzuzeigen, müssen Sie im Befehl das Argument `sp` angeben.

- `Administration Server certificate` – Parameter zur Angabe, ob das Client-Gerät über ein Zertifikat des Administrationsservers verfügt. Es kann beispielsweise vorkommen, das kein Zertifikat vorhanden ist, wenn sich der Administrationsagent noch nie erfolgreich mit dem Administrationsserver verbunden hat.

  Mögliche Werte:

  - `not installed` – Das Client-Gerät besitzt kein Zertifikat des Administrationsservers.
  - `available` –Das Client-Gerät besitzt ein Zertifikat des Administrationsservers.

- `Open UDP port` – Parameter zur Angabe, ob der Administrationsagent den UDP-Port verwendet, um Synchronisierungsanfragen vom Administrationsserver zu empfangen.

  Mögliche Werte:

  - 0 – Der UDP-Port ist für den Empfang von Synchronisationsanfragen vom Administrationsserver geschlossen.
  - 1 – Der UDP-Port ist für den Empfang von Synchronisationsanfragen vom Administrationsserver geöffnet.

- `Numbers of UDP ports` – Nummern der UDP-Ports, die vom Administrationsagenten verwendet werden können.
- `Location name` – Netzwerkstandort des Geräts.
- `State of network location` – Parameter zu Angabe, ob auf dem Client-Gerät von einem Administrationsserver-Verbindungsprofil auf ein anderes gewechselt werden kann.

  Mögliche Werte:

  - `Enabled` – Das Administrationsserver-Verbindungsprofil kann für das Client-Gerät gewechselt werden.
  - `Disabled` – Das Administrationsserver-Verbindungsprofil kann für das Client-Gerät nicht gewechselt werden.

- `Profile to use` – Verbindungsprofil für den Administrationsserver.
- `Condition` – IP-Adresse und Subnetzmaske des Netzwerks, mit dem das Client-Gerät verbunden ist.
- `Synchronization interval (min)` –Standardintervall zwischen Synchronisierungen.
- `Connection timeout (in seconds)` – Timeout für die Verbindung.
- `Send / receive timeout (in seconds)` – Timeout für die Verbindung von Lese-/Schreibvorgängen.
- `Device ID` – Geräte-ID im Netzwerk. Die `Device ID` ist für jedes Client-Gerät eindeutig, das von einem bestimmten Administrationsserver verwaltet wird.
- `Locations of connection gateways` – Parameter für die Verbindung des Client-Geräts mit dem Administrationsserver über das Verbindungs-Gateway.
- `Location of distribution points` – Parameter für die Verbindung des Client-Geräts mit dem Administrationsserver über den Verteilungspunkt.
- `Connection with server` –Parameter zur Angabe, ob das Verbindungs-Gateway eine dauerhafte Verbindung zum Administrationsserver unterhält. Der Parameter wird nur angezeigt, wenn das Client-Gerät als Verbindungs-Gateway agiert.

Mögliche Werte:

- `active` – Das Verbindungs-Gateway unterhält eine dauerhafte Verbindung zum Administrationsserver.
- `inactive` – Das Verbindungs-Gateway unterhält keine dauerhafte Verbindung zum Administrationsserver.

- `Connection with server through connection gateway` – Parameter zur Angabe, ob die Verbindung zum Administrationsserver über ein Verbindungs-Gateway korrekt hergestellt wurde. Der Parameter wird nur angezeigt, wenn das Client-Gerät als Verbindungs-Gateway agiert.

  Mögliche Werte:

  - `active` – Die Verbindung zum Administrationsserver über ein Verbindungs-Gateway wurde ordnungsgemäß hergestellt.
  - `inactive` – Die Verbindung zum Administrationsserver über ein Verbindungs-Gateway wurde nicht ordnungsgemäß hergestellt.

Darüber hinaus kann die Ausgabe des Tools "klnagchk" eine der folgenden Zeilen enthalten:

- `Administration Server is installed on this device` – Das Tool "klnagchk" wird auf dem Gerät mit dem Administrationsserver ausgeführt.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server` – Das Tool "klnagchk" wird auf einem Gerät ausgeführt, auf dem der Administrationsagent im Verbindungs-Gateway-Modus installiert ist. Das konfigurierte Verbindungs-Gateway wartet auf eine Verbindung vom Administrationsserver, aber dieser listet das Gerät nicht unter den verwalteten Geräten auf. Sie müssen sicherstellen, dass der Administrationsserver eine Verbindung zu dem Verbindungs-Gateway initiiert.
- `This device is a connection gateway` –Das Tool "klnagchk" wird auf einem Gerät ausgeführt, das als Verbindungs-Gateway agiert.
- `Acts as a distribution point` – Das Tool "klnagchk" wird auf einem Gerät ausgeführt, das als Verteilungspunkt agiert.

Das Tool "klnagchk" überprüft den Status des Dienstes des Administrationsagenten. Wird dieser Dienst nicht ausgeführt, wird das Tool beendet. Wenn der Dienst ausgeführt wird, zeigt das Tool die folgenden Verbindungsstatistiken an:

- `Total number of synchronization requests` – Anzahl der Versuche, eine Verbindung des Client-Geräts mit dem Administrationsserver herzustellen.
- `The number of successful synchronization request` – Anzahl der erfolgreichen Versuche, eine Verbindung des Client-Geräts mit dem Administrationsserver herzustellen.
- `Total number of synchronizations` – Anzahl der Versuche, die Einstellungen des Client-Geräts mit den Einstellungen des Administrationsservers zu synchronisieren.
- `The number of successful synchronizations` – Anzahl der erfolgreichen Versuche, die Einstellungen des Client-Geräts mit dem Administrationsserver zu synchronisieren.
- `Date/time of the last request for synchronization` – Datum und Uhrzeit der letzten Verbindung.

Um die Verbindung zwischen dem Administrationsserver und dem Administrationsagenten zu analysieren, müssen Sie die Parameter `Total number of synchronization requests` und `The number of successful synchronization request` verwenden. Die Einstellungen des Client-Geräts werden nur dann mit den Einstellungen des Administrationsservers synchronisiert, wenn sich die Einstellungen des Administrationsservers geändert haben (z. B. wenn neue Aufgaben hinzugefügt oder Richtlinieneinstellungen geändert wurden). Andernfalls bleiben die Parameterwerte `Total number of synchronizations` und `The number of successful synchronizations` unverändert.

Weitere Informationen zur Behebung von Verbindungsproblemen zwischen Administrationsagenten und Administrationsserver finden Sie in den FAQ zu Kaspersky Security Center Linux.

Verschiebungsregeln für Geräte

Es wird empfohlen, die Verteilung von Geräten auf Administrationsgruppen mithilfe der *Regeln für das Verschieben von Geräten* zu automatisieren. Die Regel zum Verschieben besteht aus drei Hauptteilen: dem Namen, der Ausführungsbedingung (logischer Ausdruck über die Attribute des Geräts) und der Zieladministrationsgruppe. Die Regel verschiebt das Gerät in die Zieladministrationsgruppe, wenn die Attribute des Geräts die Bedingung für die Regelausführung erfüllen.

Alle Regeln für das Verschieben von Geräten haben Prioritäten. Der Administrationsserver prüft die Attribute des Geräts auf Übereinstimmung mit der Bedingung für die jeweilige Regelausführung in abnehmender Priorität der Regeln. Wenn die Attribute des Geräts die Bedingungen für die Regelausführung erfüllen, wird das Gerät in die Zielgruppe verschoben und beendet daraufhin die Verarbeitung der Regeln für das betreffende Gerät. Wenn die Attribute des Geräts sofort einigen Regeln entsprechen, wird das Gerät in die Zielgruppe jener Regel verschoben, welche die höchste Priorität hat (in der Liste der Regeln weiter oben steht).

Die zum Geräte verschieben können implizit erstellt werden. Beispielsweise kann in den Eigenschaften des Installationspakets oder der Aufgabe zur Remote-Installation die Administrationsgruppe angegeben werden, in die das Gerät gelangen soll, nachdem darauf der Administrationsagent installiert wurde. Regeln zum Verschieben von Geräten kann der Administrator von Kaspersky Security Center Linux auch explizit im Abschnitt **Asset-Verwaltung → Verschiebungsregeln** erstellen.

Die Regel zum Verschiebung ist standardmäßig für die einmalige erstmalige Verteilung der Geräte auf die Administrationsgruppen vorgesehen. Die Regel verschiebt die Geräte, die sich in der Gruppe für nicht zugeordnete Geräte befinden, nur einmal. Wenn ein Gerät von dieser Regel einmal verschoben wurde, wird es nicht nochmals von der Regel verschoben, selbst wenn das Gerät manuell erneut in die Gruppe für nicht zugeordnete Geräte verschoben wird. Dies ist die empfohlene Art der Nutzung der Regeln zum Verschieben.

Es können Geräte verschoben werden, die sich bereits in Administrationsgruppen befinden. Dazu muss in den Eigenschaften der Regel das Kontrollkästchen **Nur Geräte verschieben, die keiner Administrationsgruppe angehören** deaktiviert werden.

Durch die Existenz von Regeln zum Verschieben, die auf Geräte gelten, die bereits in die Administrationsgruppen verschoben wurden, steigt die Belastung auf dem Administrationsserver erheblich.

In den Eigenschaften von automatisch erstellten Verschiebungsregeln ist das Kontrollkästchen **Nur Geräte verschieben, die keiner Administrationsgruppe angehören** gesperrt. Diese Regeln werden erstellt, wenn Sie die Aufgabe *Remote-Installation einer Anwendung* hinzufügen oder ein autonomes Installationspaket erstellen.

Es kann eine Regel zum Verschieben erstellt werden, die auf einem Gerät mehrfach ausgeführt werden kann.

Es wird dringend empfohlen, Szenarien zu vermeiden, bei denen ein verwaltetes Gerät mehrfach aus einer Gruppe in eine andere verschoben wird (z. B. um eine besondere Richtlinie auf das Gerät anzuwenden, eine spezielle Gruppenaufgabe zu starten oder das Gerät über einen bestimmten Verteilungspunkt zu aktualisieren).

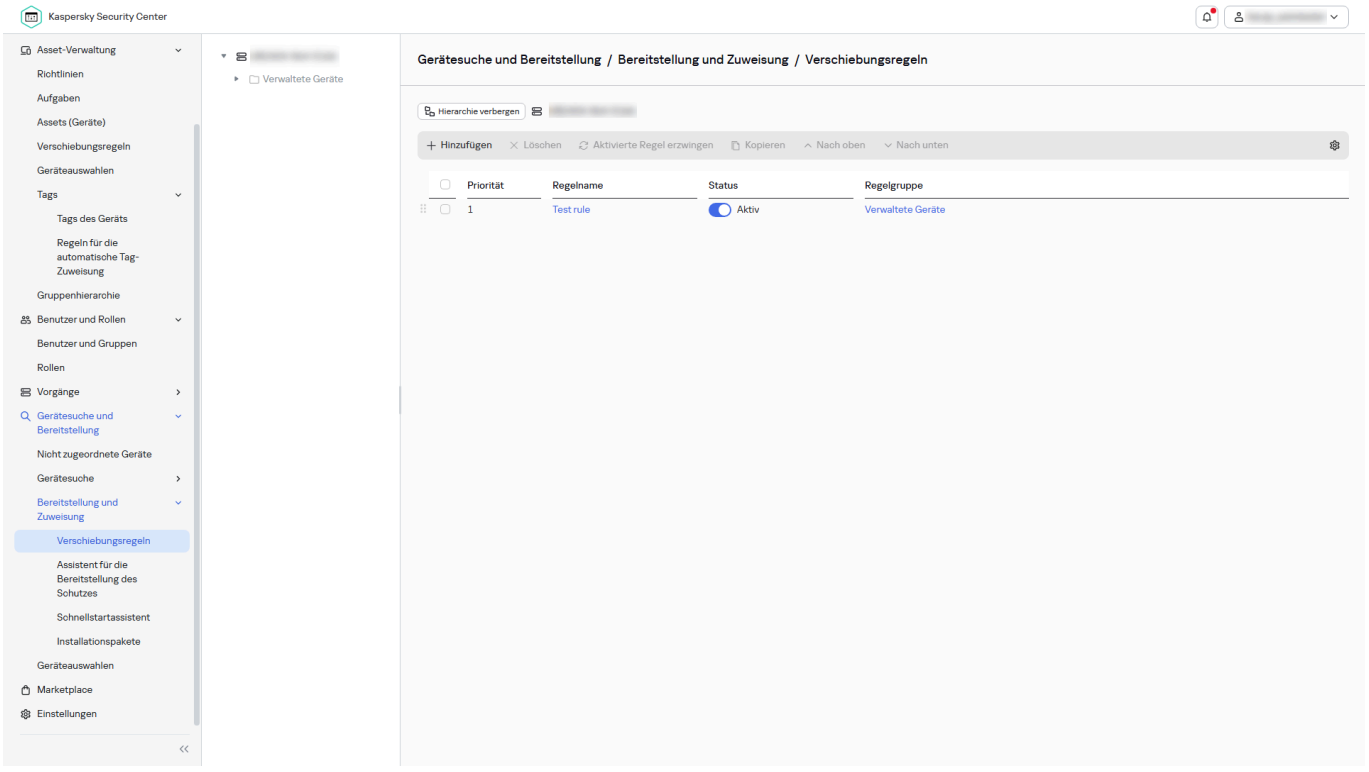
Solche Szenarien werden nicht unterstützt, da sie die Belastung des Administrationsservers und den Datenverkehr in extremem Ausmaß erhöhen. Diese Szenarien stehen ferner in Konflikt mit den Betriebsprinzipien von Kaspersky Security Center Linux (insbesondere im Bereich von Zugriffsrechen, Ereignissen und Berichten). Es müssen andere Lösungen gesucht werden, zum Beispiel durch Verwendung der Richtlinienprofile, der Aufgaben für Geräteauswahlen und der Zuweisung von Administrationsagenten entsprechend dem Standardszenario.

Regeln für das Verschieben von Geräten erstellen

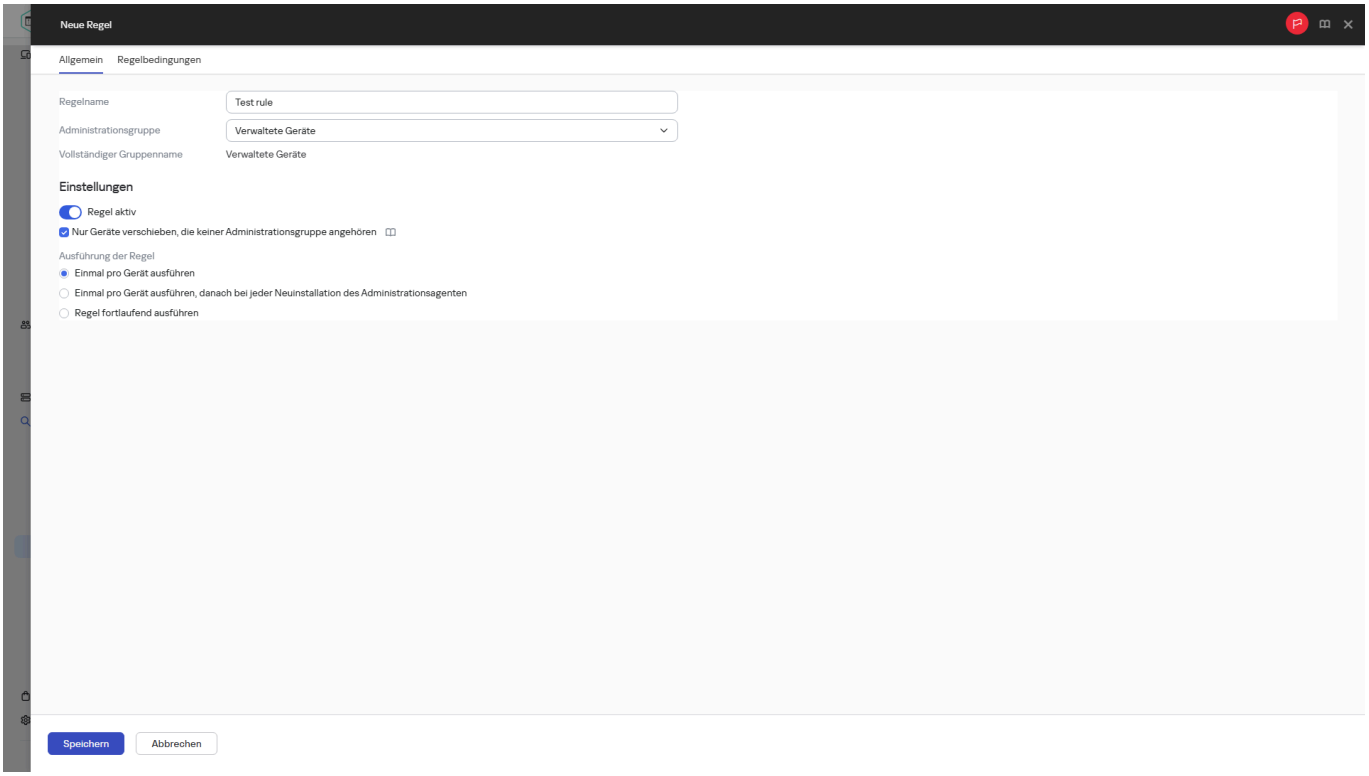
Sie können Verschiebungsregeln für Geräte einrichten, welche die Geräte automatisch den Administrationsgruppen zuzuordnen.

Um eine Verschiebungsregel zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Verschiebungsregeln**.



2. Klicken Sie auf **Hinzufügen**. Das Fenster **Neue Regel** wird geöffnet.



3. Geben Sie im nächsten Fenster auf der Registerkarte **Allgemein** die folgenden Informationen an:

- **Regelname**

  Geben Sie einen Namen für die neue Regel ein.

  Wenn Sie eine Regel kopieren, erhält die neue Regel denselben Namen wie die ursprüngliche Regel, aber der Name wird um einen Index im Format () erweitert – z. B. (1).

- **Administrationsgruppe**

  Wählen Sie die Administrationsgruppe aus, in welche die Geräte automatisch verschoben werden sollen.

- **Aktive Regel**

  Wenn diese Option aktiviert ist, wird die Regel aktiviert und ab dem Speicherzeitpunkt berücksichtigt.

  Wenn diese Option deaktiviert ist, wird die Regel erstellt, aber nicht aktiviert. Sie wird erst berücksichtigt, sobald Sie diese Option aktivieren.

- **Priorität**

  Sie können die Priorität der zu verschiebenden Regel festlegen. Der Wert "1" entspricht der höchsten Priorität. Je größer der **Priorität**, desto niedriger ist die Priorität der Regel und ihre Position in der Liste.

  Wenn keine Priorität zugewiesen ist, wird der Regel die niedrigste Priorität zugewiesen.

  Wenn eine Regel kopiert wird, wird der Kopie die Priorität der Originalregel zugewiesen. Die Priorität der Originalregel wird in diesem Fall um 1 erhöht.

- **Nur Geräte verschieben, die keiner Administrationsgruppe angehören**

  Wenn diese Option aktiviert ist, werden nur nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

Wenn diese Option deaktiviert ist, werden Geräte, die bereits zu anderen Administrationsgruppen gehören, sowie nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

- **Ausführung der Regel**

  Sie können eine der folgenden Varianten auswählen:

  - **Einmal pro Gerät ausführen**

    Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt.

  - **Einmal pro Gerät ausführen, danach bei jeder Neuinstallation des Administrationsagenten**

    Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt, und danach nur bei Neuinstallation des Administrationsagenten auf diesen Geräten.

  - **Regel fortlaufend ausführen**

    Die Regel wird gemäß einem Zeitplan angewendet, der automatisch vom Administrationsserver festgelegt wird (in der Regel alle paar Stunden).

4. Definieren Sie auf der Registerkarte **Regelbedingungen** mindestens ein Kriterium, nach dem die Geräte in eine Administrationsgruppe verschoben werden.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Verschiebungsregel wird erstellt. Sie wird in der Liste der Verschiebungsregeln angezeigt.

Je höher ihre Position in der Liste ist, desto höher ist die Priorität der Regel.

So ändern Sie die Priorität:

1. Aktivieren Sie das Kontrollkästchen einer zu verschiebenden Regel.
2. Führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf die Schaltfläche **Priorität ändern** und geben Sie anschließend die neue Priorität an.
   - Verschieben Sie die Regel in der Liste nach oben oder unten, indem Sie die entsprechenden Schaltflächen **Nach oben** oder **Nach unten** anklicken.
3. Klicken Sie auf die Schaltfläche **Speichern**.

> Wenn die Option **Regel fortlaufend ausführen** ausgewählt ist, wird die Verschiebungsregel unabhängig von der eingestellten Priorität angewendet. Diese Regeln werden gemäß einem Zeitplan angewendet, der automatisch vom Administrationsserver erstellt wird.

Wenn die Attribute des Geräts sofort einigen Regeln entsprechen, wird das Gerät in die Zielgruppe jener Regel verschoben, welche die höchste Priorität hat (in der Liste der Regeln weiter oben steht).

Regeln für das Verschieben von Geräten kopieren

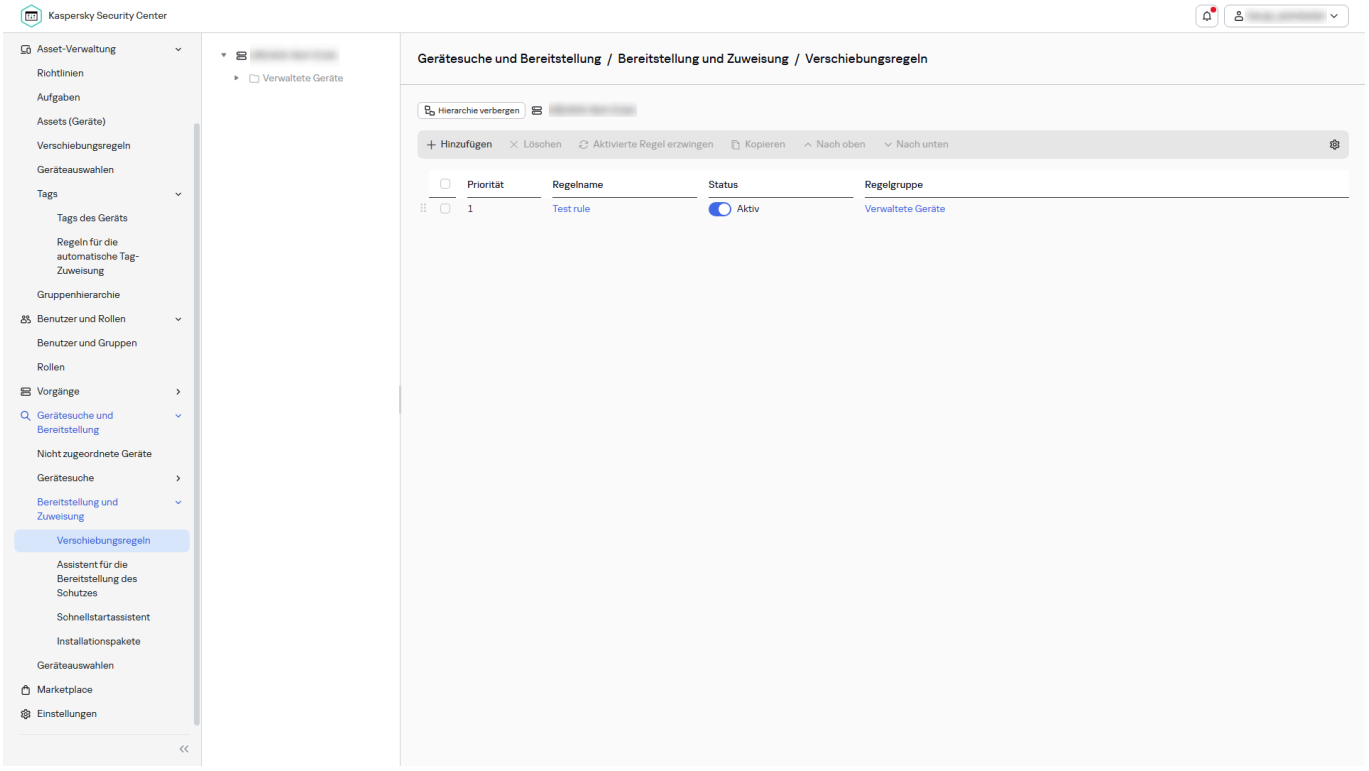
Sie können Verschiebungsregeln kopieren, wenn Sie zum Beispiel mehrere identische Regeln für verschiedene Administrationszielgruppen haben möchten.

Um eine Verschiebungsregel zu kopieren, gehen Sie wie folgt vor:

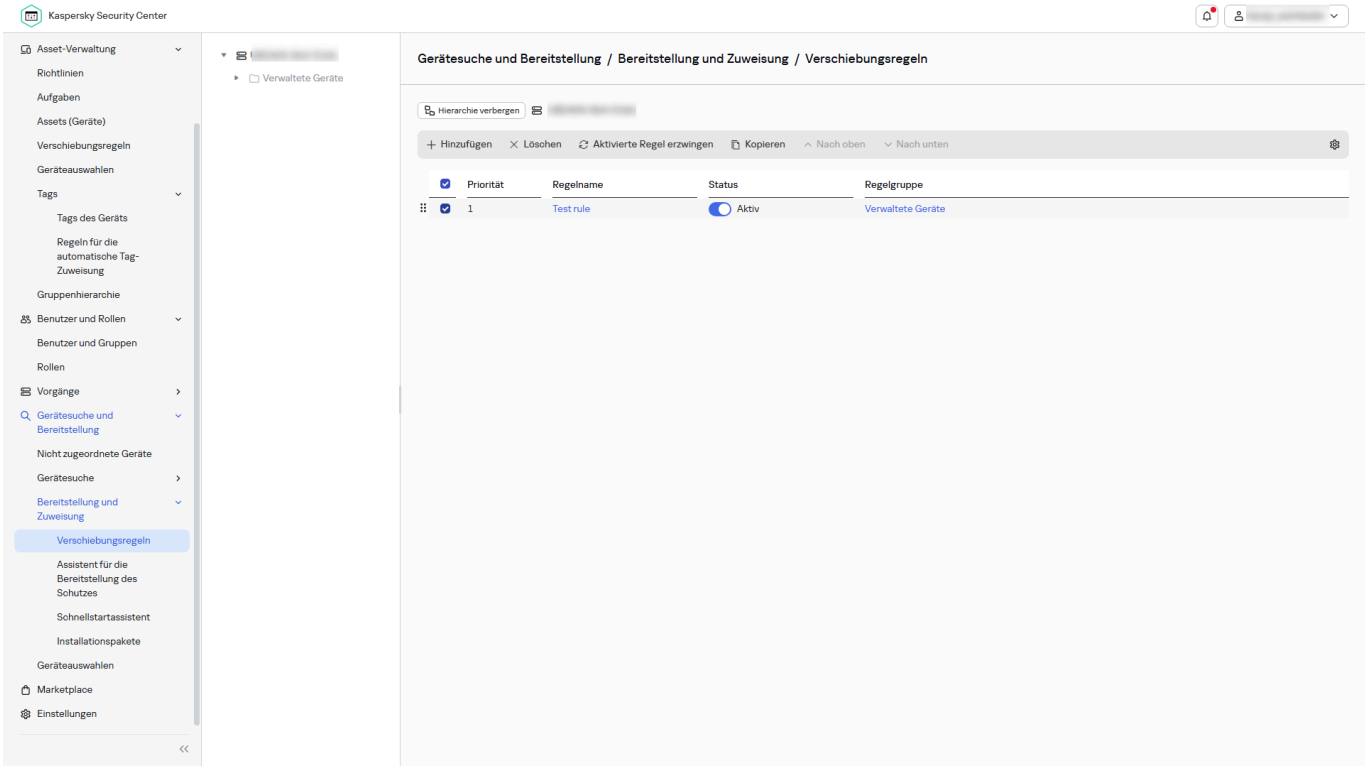
1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Verschiebungsregeln**.
   - Gehen Sie im Hauptmenü zu **Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Verschiebungsregeln**.

   Die Liste mit Verschiebungsregeln wird angezeigt.



2. Aktivieren Sie das Kontrollkästchen neben der Regel, die Sie kopieren möchten.



3. Klicken Sie auf die Schaltfläche **Kopieren**.

4. Passen Sie im nächsten Fenster die folgenden Informationen auf der Registerkarte **Allgemein** an oder belassen Sie diese, wie sie sind, wenn Sie die Regel unverändert kopieren möchten:

   - **Regelname**

     Geben Sie einen Namen für die neue Regel ein.

     Wenn Sie eine Regel kopieren, erhält die neue Regel denselben Namen wie die ursprüngliche Regel, aber der Name wird um einen Index im Format () erweitert – z. B. (1).

   - **Administrationsgruppe**

     Wählen Sie die Administrationsgruppe aus, in welche die Geräte automatisch verschoben werden sollen.

   - **Aktive Regel**

     Wenn diese Option aktiviert ist, wird die Regel aktiviert und ab dem Speicherzeitpunkt berücksichtigt.

     Wenn diese Option deaktiviert ist, wird die Regel erstellt, aber nicht aktiviert. Sie wird erst berücksichtigt, sobald Sie diese Option aktivieren.

   - **Priorität**

     Sie können die Priorität der zu verschiebenden Regel festlegen. Der Wert "1" entspricht der höchsten Priorität. Je größer der **Priorität**, desto niedriger ist die Priorität der Regel und ihre Position in der Liste.

     Wenn keine Priorität zugewiesen ist, wird der Regel die niedrigste Priorität zugewiesen.

     Wenn eine Regel kopiert wird, wird der Kopie die Priorität der Originalregel zugewiesen. Die Priorität der Originalregel wird in diesem Fall um 1 erhöht.

   - **Nur Geräte verschieben, die keiner Administrationsgruppe angehören**

     Wenn diese Option aktiviert ist, werden nur nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

     Wenn diese Option deaktiviert ist, werden Geräte, die bereits zu anderen Administrationsgruppen gehören, sowie nicht zugeordnete Geräte in die ausgewählte Gruppe verschoben.

   - **Ausführung der Regel**

     Sie können eine der folgenden Varianten auswählen:

     - **Einmal pro Gerät ausführen**

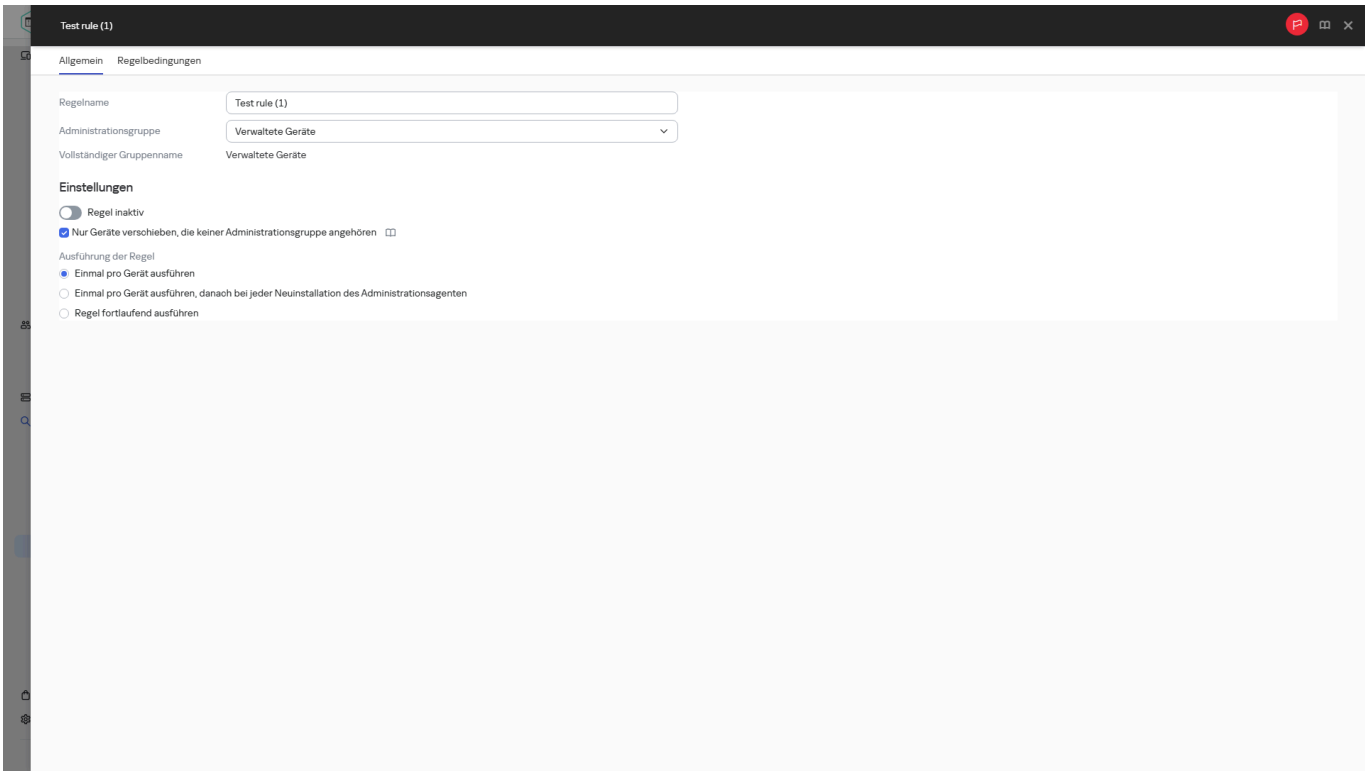
       Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt.

     - **Einmal pro Gerät ausführen, danach bei jeder Neuinstallation des Administrationsagenten**

       Die Regel wird für jedes Gerät, das Ihren Kriterien entspricht, einmal ausgeführt, und danach nur bei Neuinstallation des Administrationsagenten auf diesen Geräten.

     - **Regel fortlaufend ausführen**

       Die Regel wird gemäß einem Zeitplan angewendet, der automatisch vom Administrationsserver festgelegt wird (in der Regel alle paar Stunden).



5. Definieren Sie auf der Registerkarte **Regelbedingungen** mindestens ein Kriterium für die Geräte, die automatisch verschoben werden sollen.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Die neue Verschiebungsregel wird erstellt. Sie wird in der Liste der Verschiebungsregeln angezeigt.

Bedingungen für Verschiebungsregeln für Geräte

Wenn Sie eine Regel erstellen oder kopieren, um Client-Geräte in Administrationsgruppen zu verschieben, geben Sie auf der Registerkarte **Regelbedingungen** die Bedingungen zum Verschieben der Geräte an. Um festzulegen, welche Geräte verschoben werden sollen, können Sie die folgenden Kriterien verwenden:

- Den Client-Geräten zugewiesene Tags.
- Netzwerkparameter. Beispielsweise können Sie Geräte mit IP-Adressen aus einem bestimmten Bereich verschieben.
- Verwaltete Anwendungen, die auf Client-Geräten installiert sind, z. B. Administrationsagent oder Administrationsserver.
- Client-Geräte, die virtuelle Maschinen sind.

Nachfolgend finden Sie die Beschreibung, wie Sie diese Informationen in Verschiebungsregeln für Geräte angeben.

Wenn Sie in der Regel mehrere Bedingungen, werden alle mittels logischem UND-Operator verknüpft und alle Bedingungen gelten gleichzeitig. Wenn Sie gar keine Optionen auswählen oder einige Felder leer lassen, gelten diese Bedingungen nicht.

Registerkarte Tags

Auf dieser Registerkarte können Sie eine Verschiebungsregel für Geräte basierend auf Geräte-Tags anpassen, die den Beschreibungen der Client-Geräte zuvor hinzugefügt wurden. Wählen Sie dazu die erforderlichen Tags aus. Darüber hinaus können Sie die folgenden Optionen aktivieren:

- **Gilt für Geräte ohne die angegebenen Tags**

  Wenn diese Option aktiviert ist, werden alle Geräte mit den angegebenen Tags von einer Verschiebungsregel ausgeschlossen. Wenn diese Option deaktiviert ist, gilt die Verschiebungsregel für Geräte mit allen ausgewählten Tags.

  Diese Option ist standardmäßig deaktiviert.

- **Anwenden, wenn mindestens eins der ausgewählten Tags zutrifft**

  Wenn diese Option aktiviert ist, gilt eine Verschiebungsregel für Client-Geräte mit mindestens einem der ausgewählten Tags. Wenn diese Option deaktiviert ist, gilt die Verschiebungsregel für Geräte mit allen ausgewählten Tags.

  Diese Option ist standardmäßig deaktiviert.

Registerkarte Netzwerk

Auf dieser Registerkarte können Sie die Netzwerkdaten von Geräten angeben, die eine Verschiebungsregel für Geräte berücksichtigt:

- **Gerätename im Windows-Netzwerk**

  Windows-Netzwerkname (NetBIOS-Name) des Geräts oder die IPv4- oder IPv6-Adresse.

- **DNS-Name des Geräts**

  Name der DNS-Domänen des Client-Geräts, das Sie verschieben möchten. Füllen Sie dieses Feld aus, wenn Ihr Netzwerk einen DNS-Server enthält.

  > Wenn für die Datenbank, die Sie für Kaspersky Security Center Linux verwenden, die Kollation zwischen Groß- und Kleinschreibung festgelegt ist, behalten Sie die Groß-/Kleinschreibung bei, wenn Sie einen DNS-Namen für das Gerät angeben. Andernfalls funktioniert die Verschiebungsregel für Geräte nicht.

- **DNS-Domäne**

  Eine Verschiebungsregel gilt für alle Geräte, die im angegebenen primären DNS-Suffix enthalten sind. Füllen Sie dieses Feld aus, wenn Ihr Netzwerk einen DNS-Server enthält.

- **IP-Bereich**

  Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern die erste und die letzte IP-Adresse des Bereichs eingeben, zu dem die betreffenden Geräte gehören sollen.

  Diese Option ist standardmäßig deaktiviert.

- **IP-Adresse für die Verbindung mit dem Administrationsserver**

  Wenn diese Option aktiviert ist, können Sie die IP-Adressen festlegen, über die Client-Geräte mit dem Administrationsserver verbunden werden. Geben Sie dazu den IP-Bereich an, der alle notwendigen IP-Adressen enthält.

Diese Option ist standardmäßig deaktiviert.

- **Gerät befindet sich im IP-Bereich**

  Wenn diese Option aktiviert ist, können Sie einen IP-Bereich auswählen, den Sie im Abschnitt **IP-Bereiche** zuvor hinzugefügt haben. Die betreffenden Geräte müssen im gewählten IP-Bereich enthalten sein.

  Diese Option ist standardmäßig deaktiviert.

- **Verbindungsprofil wurde geändert**

  Wählen Sie eine der folgenden Werte aus:

  - **Ja**. Eine Verschiebungsregel gilt nur für Client-Geräte mit einem geänderten Verbindungsprofil.
  - **Nein**. Die Verschiebungsregel gilt nur für Client-Geräte, deren Verbindungsprofile sich nicht geändert haben.
  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

- **Verwaltung erfolgt durch anderen Administrationsserver**

  Wählen Sie eine der folgenden Werte aus:

  - **Ja**. Eine Verschiebungsregel gilt nur für Client-Geräte, die von anderen Administrationsservern verwaltet werden. Diese Server unterscheiden sich von dem Server, auf dem Sie die Verschiebungsregel für Geräte konfigurieren.
  - **Nein**. Die Verschiebungsregel gilt nur für Client-Geräte, die vom aktuellen Administrationsserver verwaltet werden.
  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

Registerkarte Gerätebesitzer

Auf dieser Registerkarte können Sie eine Regel zum Verschieben von Geräten basierend auf dem Gerätebesitzer, der Sicherheitsgruppenmitgliedschaft und der Rolle konfigurieren:

- **Gerätebesitzer**

  Wählen Sie den Benutzernamen des Gerätebesitzers aus einer internen Sicherheitsgruppe aus. Weitere Informationen über Benutzer und Benutzerrollen finden Sie in diesem Abschnitt.

  > Es kann nur ein Benutzer als Gerätebesitzer registriert sein.

- **Zugehörigkeit des Gerätebesitzers zu einer Active Directory-Sicherheitsgruppe**

  Wählen Sie eine externe Active Directory-Sicherheitsgruppe aus, welcher der Gerätebesitzer angehört.

  > Der Benutzer kann entweder Teil einer Active Directory-Sicherheitsgruppe oder Teil einer Gruppe sein, die selbst zu der ausgewählten Active Directory-Sicherheitsgruppe gehört.

- **Rolle des Gerätebesitzers**

  Wählen Sie die Rolle aus, die dem Gerätebesitzer zugewiesen ist. Weitere Informationen über Benutzerrollen finden Sie in diesem Artikel.

- **Zugehörigkeit des Gerätebesitzers zu einer internen Sicherheitsgruppe**

  Wählen Sie eine interne Sicherheitsgruppe aus, welcher der Gerätebesitzer angehört.

Registerkarte Anwendungen

Auf dieser Registerkarte können Sie eine Regel zum Verschieben von Geräten basierend auf den verwalteten Anwendungen und Betriebssystemen konfigurieren, die auf Client-Geräten installiert sind:

- **Administrationsagent ist installiert**

  Wählen Sie eine der folgenden Werte aus:

  - **Ja**. Eine Verschiebungsregel gilt nur für Client-Geräte, auf denen der Administrationsagent installiert ist.
  - **Nein**. Die Verschiebungsregel gilt nur für Client-Geräte, auf denen der Administrationsagent nicht installiert ist.
  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

- **Anwendungen**

  Geben Sie an, welche verwalteten Anwendungen auf Client-Gerät installiert sein müssen, damit für diese Geräte eine Verschiebungsregel gilt. Sie können beispielsweise **Kaspersky Security Center 16.3 Administrationsagent** oder **Kaspersky Security Center 16.3 Administrationsserver** angeben.

  Wenn Sie keine verwaltete Anwendung auswählen, trifft die Bedingung nicht zu.

- **Aktiviert**

  Sie können Client-Geräte basierend auf deren Betriebssystemversionen auswählen. Geben Sie dazu Betriebssysteme an, die auf den Client-Geräten installiert sein müssen. Als Ergebnis gilt eine Verschiebungsregeln für die Client-Geräte mit den ausgewählten Betriebssystemen.

  Wenn Sie diese Option nicht aktivieren, trifft die Bedingung nicht zu. Die Option ist standardmäßig deaktiviert.

- **Architektur des Betriebssystems**

  Sie können Client-Geräte anhand der Bitanzahl des Betriebssystems auswählen. Im Block **Architektur des Betriebssystems** können Sie einen der folgenden Werte auswählen:

  - **Unbekannt**
  - **x86**
  - **AMD64**
  - **IA64**

  So überprüfen Sie die Bitanzahl des Betriebssystems der Client-Geräte:

  1. Gehen Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung → Assets (Geräte)**.
  2. Klicken Sie auf die Schaltfläche **Spalteneinstellungen** (⚙) auf der rechten Seite.

3. Aktivieren Sie die Option **Architektur des Betriebssystems** und klicken Sie anschließend auf die Schaltfläche **Speichern**.

   Danach wird die Bitanzahl des Betriebssystems für jedes verwaltete Gerät angezeigt.

- **Paketverwaltung des Betriebssystems**

  Sie können Client-Geräte über den Paketmanager des Betriebssystems auswählen. Im **Paketverwaltung des Betriebssystems**-Feld können Sie einen der folgenden Werte auswählen:

  - rpm – für Geräte, auf denen die Betriebssysteme Red Hat Enterprise Linux, CentOS, Fedora, SUSE und Oracle Linux laufen
  - apt (dpkg) – für Geräte, auf denen die Betriebssysteme Debian-, Ubuntu und Kali laufen
  - pkg – für Geräte, auf denen die Betriebssysteme FreeBSD und OpenBSD laufen

  So überprüfen Sie den Paketmanager des Betriebssystems der Client-Geräte:

  1. Gehen Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung** → **Assets (Geräte)**.
  2. Klicken Sie auf die Schaltfläche **Spalteneinstellungen** (⚙) auf der rechten Seite.
  3. Wählen Sie die **Paketverwaltung des Betriebssystems**-Option und klicken Sie dann auf die **Speichern**-Schaltfläche.

  Der Paketmanager des Betriebssystems wird für jedes verwaltete Gerät angezeigt.

- **Architektur des Betriebssystems**

  In diesem Feld können Sie die Service Pack-Version (im Format *X.Y*) des Betriebssystems angeben, die bestimmt, wie die Verschiebungsregel auf das Gerät angewendet wird. Standardmäßig ist keine Version angegeben.

- **Benutzerzertifikat**

  Wählen Sie eine der folgenden Werte aus:

  - **Installiert**. Eine Verschiebungsregel gilt nur für mobile Geräte mit einem Mobilgerät-Zertifikat.
  - **Nicht installiert**. Die Verschiebungsregel gilt nur für mobile Geräte ohne Mobilgerät-Zertifikat.
  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

- **Aktiviert**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Versionsnummer haben muss. Sie können auch eine Verschiebungsregel für Geräte für alle Versionsnummern mit Ausnahme der angegebenen anpassen.

- **Aktiviert**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Release-Nummer haben muss. Sie können auch eine Verschiebungsregel für Geräte für allen Versionsnummern mit Ausnahme der angegebenen anpassen.

Registerkarte Virtuelle Maschinen

Auf dieser Registerkarte können Sie die Verschiebungsregel für Geräte anpassen, je nachdem, ob die Client-Geräte virtuelle Maschinen sind oder zur Virtual Desktop Infrastructure (VDI) gehören:

- **Ist eine virtuelle Maschine**

  In der Dropdown-Liste können Sie einen der folgenden Werte auswählen:
  - **N/A**. Die Bedingung trifft nicht zu.
  - **Nein**. Geräte verschieben, die keine virtuellen Maschinen sind.
  - **Ja**. Geräte verschieben, die virtuellen Maschinen sind.

- **Typ der virtuellen Maschine**

- **Gehört zur Virtual Desktop Infrastructure (VDI)**

  In der Dropdown-Liste können Sie einen der folgenden Werte auswählen:
  - **N/A**. Die Bedingung trifft nicht zu.
  - **Nein**. Geräte verschieben, die keine Teil einer VDI sind.
  - **Ja**. Geräte verschieben, die Teil einer VDI sind.

Registerkarte Domänencontroller

Auf dieser Registerkarte können Sie angeben, dass Geräte verschoben werden sollen, die in der Domänen-Organisationseinheit enthalten sind. Sie können auch Geräte aus allen untergeordneten Organisationseinheiten der angegebenen Domänen-Organisationseinheit verschieben:

- **Das Gerät befindet sich in folgender Organisationseinheit**

  Wenn diese Option aktiviert ist, gilt eine Verschiebungsregel für die Geräte aus dem Domänencontroller, die in der Liste unter der Option angegeben ist.

  Diese Option ist standardmäßig deaktiviert.

- **Untergeordnete Organisationseinheiten einschließen**

  Wenn die Option aktiviert ist, werden in die Auswahl alle Geräte aufgenommen, die zu einer untergeordneten Organisationseinheit des angegebenen Domänencontrollers gehören.

  Diese Option ist standardmäßig deaktiviert.

- **Geräte aus untergeordneten Organisationseinheiten in entsprechende Untergruppen verschieben**

- **Untergruppen erstellen, die Containern von neu erkannten Geräten entsprechen**

- **Untergruppen löschen, die in der Domäne fehlen**

- **Das Gerät ist Mitglied der folgenden Domänen-Sicherheitsgruppe**

  Wenn diese Option aktiviert ist, gilt eine Verschiebungsregel für die Geräte aus der Domänensicherheitsgruppe, die in der Liste unter der Option angegeben ist.

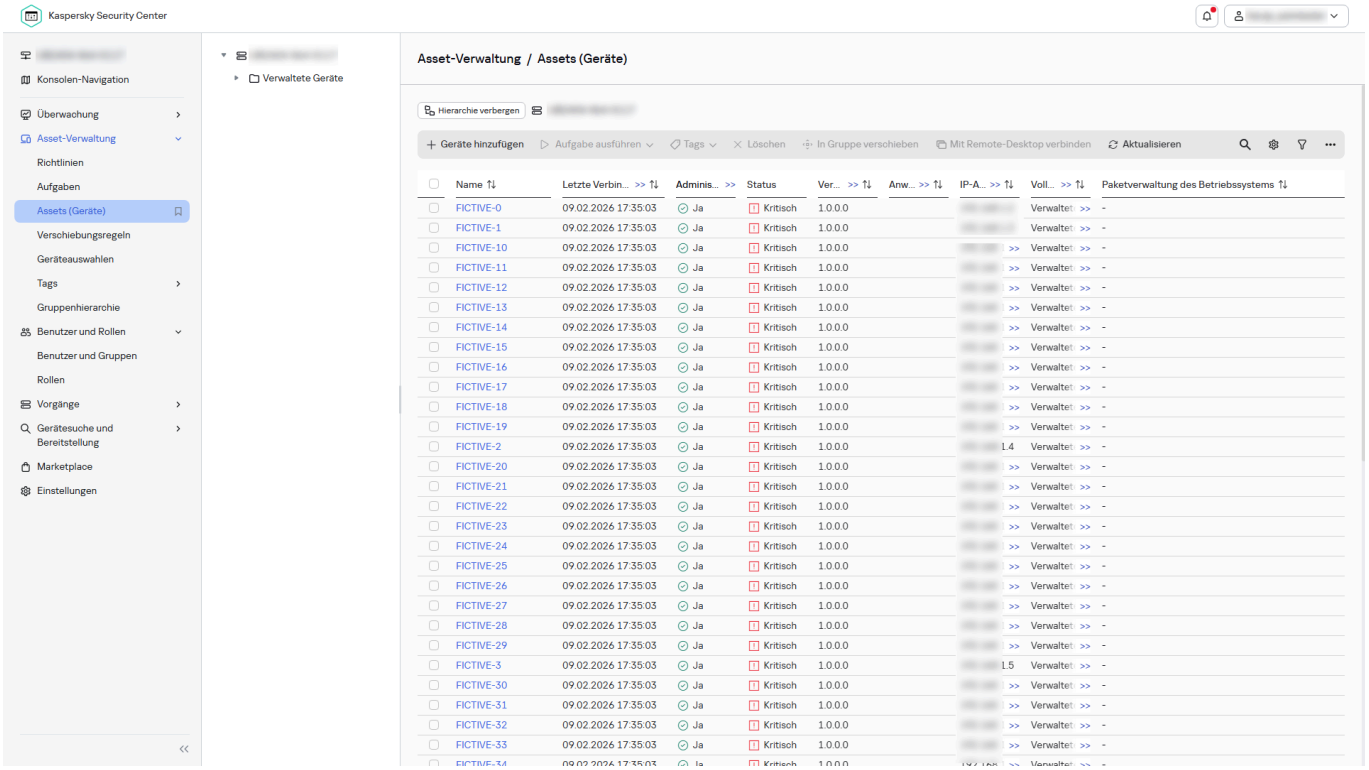
  Diese Option ist standardmäßig deaktiviert.

Geräte manuell zu einer Administrationsgruppe hinzufügen

Sie können Geräte automatisch in Administrationsgruppen verschieben, indem Sie Regeln zum Verschieben von Geräten erstellen oder manuell Geräte von einer Administrationsgruppe in eine andere verschieben oder Geräte einer ausgewählten Administrationsgruppe hinzufügen. Dieser Abschnitt beschreibt, wie Sie Geräte zu einer Administrationsgruppe manuell hinzufügen.

Um ein oder mehr Geräte zu einer ausgewählten Administrationsgruppe manuell hinzuzufügen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.



Die Liste der verwalteten Geräte

2. Wählen Sie die Administrationsgruppe aus, der Sie die Geräte hinzufügen möchten.

   - Für die Stammgruppe:

     In diesem Fall können Sie mit dem nächsten Schritt fortfahren.

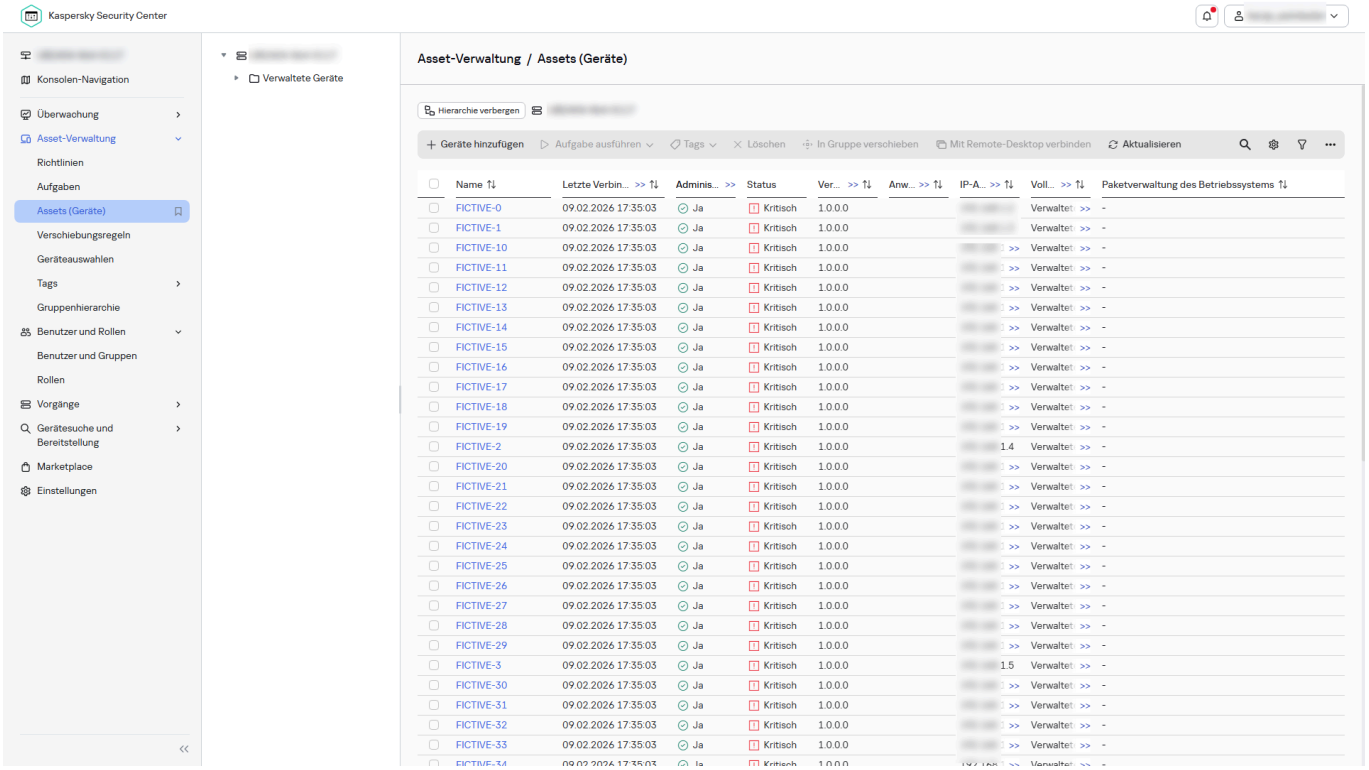
- Für eine untergeordnete Gruppe:

  a. Klicken Sie im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

  Der Name der Schaltfläche ändert sich zu **Hierarchie verbergen**.

  b. Klicken Sie im neuen Fenster auf den Namen der Untergruppe.

  Der Pfad zur ausgewählten Gruppe wird im oben Bereich der Seite angezeigt. Bei Bedarf können Sie auf einen Link mit dem Namen der Administrationsgruppe klicken, um zu dieser Gruppe zu gelangen. Der letzte Link im Pfad ist standardmäßig inaktiv. Außerdem können Sie das Hierarchiefenster schließen, indem Sie auf die Schaltfläche **Hierarchie verbergen** klicken.



Auswählen der Administrationsgruppe

3. Klicken Sie auf die Schaltfläche **Geräte hinzufügen**.

   Daraufhin wird der Assistent für das Verschieben von Geräten gestartet.

4. Erstellen Sie eine Liste mit Geräten, die Sie der Administrationsgruppe hinzufügen möchten.

   Sie können nur Geräte hinzufügen, deren Informationen bereits durch Anschließen des Geräts oder nach einer Gerätesuche in die Administrationsserver-Datenbank eingetragen wurden.

Wählen Sie aus, wie Sie Geräte zur Liste hinzufügen möchten:

- Klicken Sie auf die Schaltfläche **Geräte hinzufügen**, und geben Sie die Geräte auf eine der folgenden Arten an:
  - Wählen Sie Geräte aus der Liste der vom Administrationsserver erkannten Geräte aus.
  - Geben Sie eine IP-Adresse oder einen IP-Bereich an.

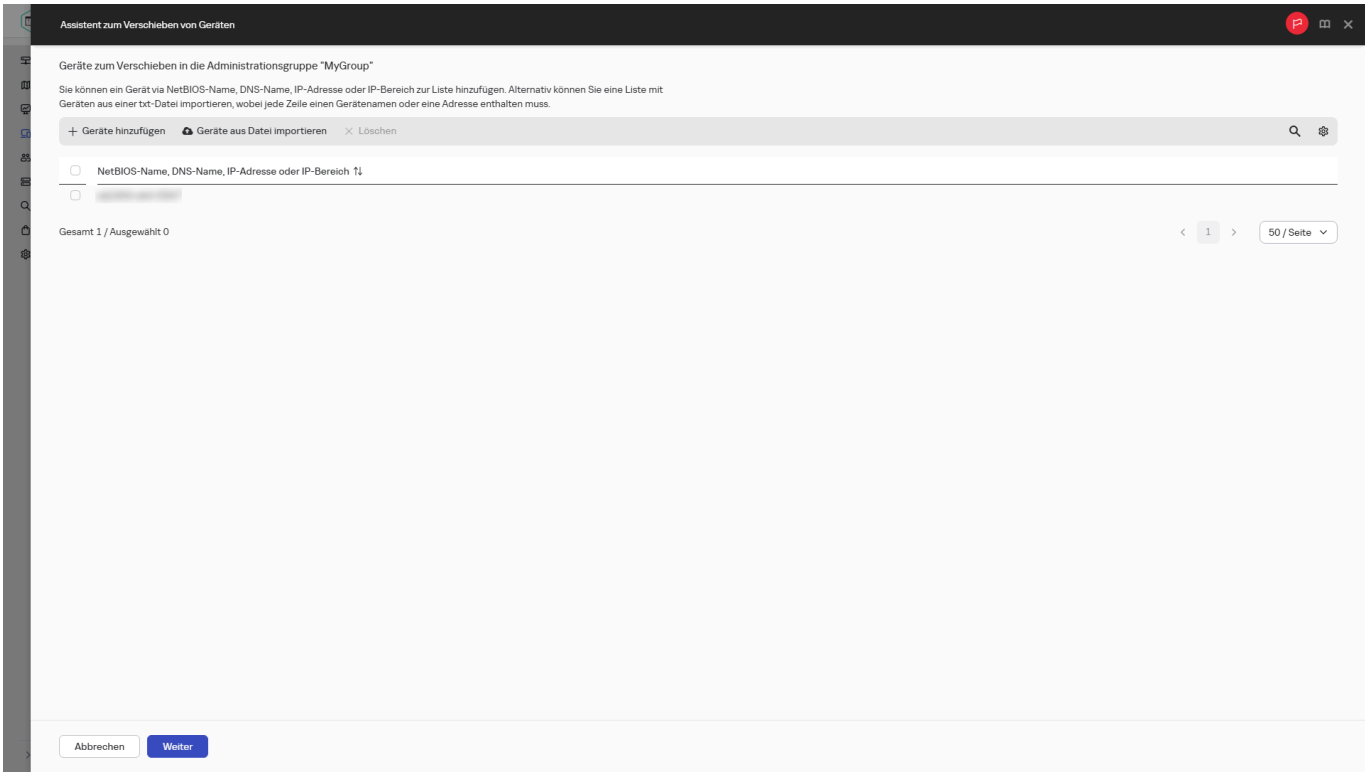
    Der IP-Bereich darf maximal 1.048.576 Adressen enthalten.

  - Geben Sie einen Geräte-DNS-Namen an.

    Das Feld für die den Gerätenamen darf keine Leerzeichen, keine Backspace-Zeichen sowie keine der folgenden verbotenen Zeichen enthalten: , \ / * ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Drücken Sie die Schaltfläche **Geräte aus Datei importieren**, um eine Liste von Geräten aus einer TXT-Datei zu importieren. Jede Adresse und jeder Name eines Gerätes müssen in einer separaten Zeile aufgeführt sein.

  Die Datei darf keine Leerzeichen, keine Backspace-Zeichen, sowie keine der folgenden verbotenen Zeichen enthalten: , \ / * ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %



Auswählen von Geräten, die in die Administrationsgruppe verschoben werden

5. Zeigen Sie die Liste der Geräte an, die der Administrationsgruppe hinzugefügt werden sollen. Sie können die Liste bearbeiten, indem Sie Geräte hinzufügen oder entfernen.

6. Wenn Sie sichergestellt haben, dass die Liste korrekt ist, klicken Sie auf die Schaltfläche **Weiter**.

Der Assistent verarbeitet die Geräteliste und zeigt das Ergebnis an. Erfolgreich verarbeitete Geräte werden der

Administrationsgruppe hinzugefügt und in der Geräteliste mit den Namen angezeigt, die der Administrationsserver bestimmt hat.

Manuelles Verschieben von Geräten oder Clustern in eine Administrationsgruppe

Sie können Geräte aus einer Administrationsgruppe in eine andere verschieben oder von der Gruppe nicht zugeordnete Geräte in eine Administrationsgruppe verschieben.

Sie können auch Cluster oder Server-Arrays von einer Administrationsgruppe in eine andere verschieben. Wenn Sie ein Cluster oder Server-Array in eine andere Gruppe verschieben, werden alle ihre Knoten mit verschoben, da ein Cluster und alle seine Knoten immer derselben Administrationsgruppe angehören. Wenn Sie auf der Registerkarte **Geräte** einen Cluster auswählen, wird die Schaltfläche **In Gruppe verschieben** inaktiv.

So verschieben Sie ein oder mehrere Geräte oder Cluster in eine ausgewählte Administrationsgruppe:

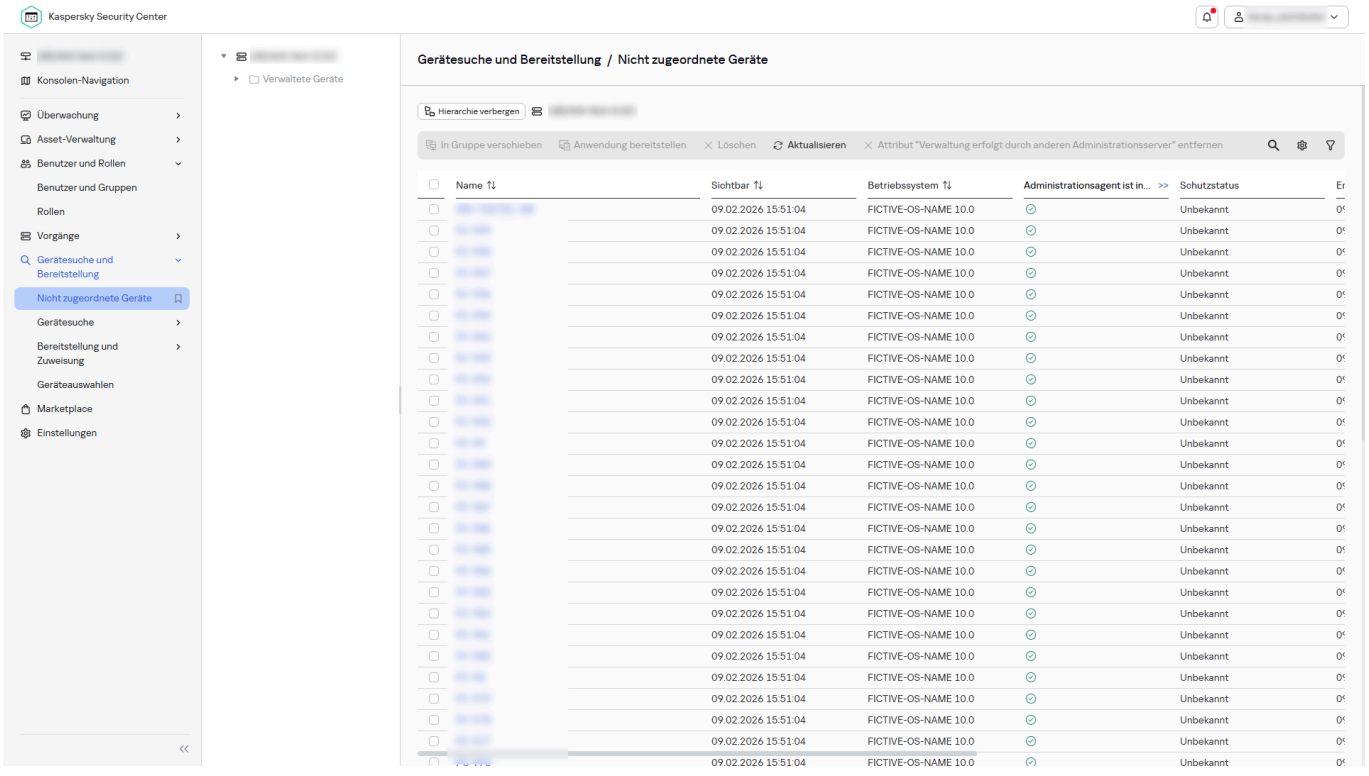
1. Öffnen Sie die Administrationsgruppe, aus welcher Sie die Geräte verschieben möchten. Führen Sie dazu eine der folgenden Aktionen aus:

   - Um eine Administrationsgruppe zu öffnen, navigieren Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte)** und wählen Sie anschließend die gewünschte Administrationsgruppe aus.

     - Für die Stammgruppe können Sie mit dem nächsten Schritt fortfahren.

     - Klicken Sie für eine Untergruppe im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen** und wählen anschließend im neuen Fenster eine erforderliche Administrationsgruppe.

   - Um die Gruppe **Nicht zugeordnete Geräte** im Hauptmenü zu öffnen, wechseln Sie zu **Asset-Verwaltung → Nicht zugeordnete Geräte**.



Die Liste der nicht zugewiesenen Geräte

2. Wenn die Administrationsgruppe Cluster oder Server-Arrays enthält, wird der Abschnitt **Assets (Geräte)** in zwei Registerkarten unterteilt – **Geräte** und **Cluster und Server-Arrays**. Öffnen Sie die Registerkarte für diese Art von Objekt, die Sie verschieben möchten.

3. Aktivieren Sie die Kontrollkästchen neben den Geräten oder Clustern, die Sie in eine andere Gruppe verschieben möchten.

4. Klicken Sie auf die Schaltfläche **In Gruppe verschieben**.

5. Aktivieren Sie in der Hierarchie der Verwaltungsgruppen das Kontrollkästchen neben der Administrationsgruppe, in welche Sie die ausgewählten Geräte oder Cluster verschieben möchten.

6. Klicken Sie auf die Schaltfläche **Verschieben**.

Die ausgewählten Geräte oder Cluster werden in die gewählte Administrationsgruppe verschoben.

Über Cluster und Server-Arrays

Kaspersky Security Center Linux unterstützt Cluster-Technologie. Sobald der Administrationsserver vom Administrationsagenten die Information erhält, dass ein auf einem Client-Gerät installiertes Programm zum Server-Array gehört, wird das betreffende Client-Gerät als Knoten in dem Cluster eingebunden.

Wenn eine Administrationsgruppe Cluster oder Server-Arrays enthält, zeigt die Seite **Assets (Geräte)** zwei Registerkarten an – eine für einzelne Geräte und eine für Cluster und Server-Arrays. Nachdem die verwalteten Geräte als Cluster-Knoten erkannt wurden, wird der Cluster als einzelnes Objekt zur Registerkarte **Cluster und Server-Arrays** hinzugefügt.

Die Knoten des Clusters oder Server-Arrays werden zusammen mit anderen verwalteten Geräten auf der Registerkarte **Geräte** angezeigt. Sie können für die Knoten wie für andere Geräte Eigenschaften anzeigen und weitere Operationen durchführen, aber Sie können einen Cluster-Knoten nicht löschen oder ihn getrennt von seinem Cluster in eine andere Administrationsgruppe verschieben. Sie können nur einen ganzen Cluster löschen oder verschieben.

Die folgenden Vorgänge können Sie mit Clustern oder Server-Arrays ausführen:

- Eigenschaften anzeigen
- Das Cluster oder Server-Array in eine andere Administrationsgruppe verschieben

  Wenn Sie ein Cluster oder Server-Array in eine andere Gruppe verschieben, werden alle ihre Knoten mit verschoben, da ein Cluster und alle seine Knoten immer derselben Administrationsgruppe angehören.

- Löschen

  Es ist nur dann sinnvoll, ein Cluster oder ein Server-Array zu löschen, wenn das Cluster oder Server-Array nicht mehr im Netzwerk der Organisation existiert. Wenn ein Cluster noch in Ihrem Netzwerk sichtbar ist und der Administrationsagent und die Kaspersky-Sicherheitsanwendung noch auf den Cluster-Knoten installiert sind, fügt Kaspersky Security Center Linux das gelöschte Cluster und seine Knoten automatisch wieder zur Liste der verwalteten Geräte hinzu.

Eigenschaften eines Cluster- oder Server-Arrays

So zeigen Sie die Einstellungen eines Clusters oder Server-Arrays an:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)** → **Cluster und Server-Arrays**.
   Die Liste der Cluster und Server-Arrays wird angezeigt.
2. Klicken Sie auf den Namen des erforderlichen Clusters oder Server-Arrays.

Das Eigenschaftenfenster des gewählten Clusters oder Server-Arrays wird geöffnet.

Allgemein

Der Abschnitt **Allgemein** zeigt allgemeine Informationen zu dem Cluster oder Server-Array an. Die Informationen beruhen auf Daten, die bei der letzten Synchronisierung der Cluster-Knoten mit dem Administrationsserver empfangen wurden:

- **Name**
- **Beschreibung**
- **Windows-Domäne**

  Windows-Domäne oder -Arbeitsgruppe, die das Cluster oder Server-Array enthält.
- **NetBIOS-Name**

  Windows-Netzwerkname des Clusters oder Server-Arrays.
- **DNS-Name**

  Name der DNS-Domäne des Clusters oder Server-Arrays.

Aufgaben

In der Registerkarte **Aufgaben** können Sie die dem Cluster oder Server-Array zugewiesenen Aufgaben verwalten: Liste der vorhandenen Aufgaben anzeigen, neue Aufgaben erstellen, Aufgaben entfernen, starten und beenden, Aufgabeneinstellungen ändern und die Ergebnisse der Aufgabenausführung anzeigen. Die aufgeführten Aufgaben beziehen sich auf die Kaspersky-Sicherheitsanwendung, die auf den Cluster-Knoten installiert ist.
Kaspersky Security Center Linux bezieht die Aufgabenliste und die Details zum Aufgabenstatus von den Cluster-Knoten. Wenn keine Verbindung hergestellt ist, wird der Status nicht angezeigt.

Knoten

Diese Registerkarte zeigt eine Liste der Knoten an, die im Cluster oder Server-Array enthalten sind. Sie können auf den Namen eines Knotens klicken, um das Fenster mit den Geräteeigenschaften anzuzeigen.

Kaspersky-Anwendung

Das Eigenschaftenfenster kann auch zusätzliche Registerkarten mit Informationen und Einstellungen bezüglich der auf den Cluster-Knoten installierten Kaspersky-Sicherheitsanwendung enthalten.

Verteilungspunkte und Verbindungs-Gateways anpassen

Die Struktur der Administrationsgruppen in Kaspersky Security Center Linux erfüllt folgende Funktionen:

- Gültigkeitsbereich der Richtlinien festlegen

  Mithilfe von *Richtlinienprofilen* existiert eine alternative Möglichkeit, um die notwendigen Einstellungen auf den Geräten anzuwenden.

- Gültigkeitsbereich der Gruppenaufgaben festlegen

  Es gibt eine Methode zur Festlegung des Gültigkeitsbereichs der Gruppenaufgaben, die nicht auf der Hierarchie der Administrationsgruppen basiert: die Nutzung von Aufgaben für die Geräteauswahlen und eine Reihe von Geräten.

- Festlegung der Zugriffsrechte auf die Geräte, sowie auf die virtuellen und sekundären Administrationsserver

- Weist Verteilungspunkte zu

Beim Aufbau der Struktur der Administrationsgruppen muss für eine optimale Bestimmung der Verteilungspunkte die Netzwerktopologie des Unternehmens berücksichtigt werden. Die optimale Zuordnung der Verteilungspunkte ermöglicht eine Verringerung des Netzwerkverkehrs innerhalb des Unternehmensnetzwerks.

Abhängig von der planmäßigen Struktur des Unternehmens und der Topologie der Netzwerke können die folgenden typischen Konfigurationen für die Struktur der Administrationsgruppen unterschieden werden:

- Einzelbüro

- Mehrere kleine, eigenständige Büros

Geräte, die als Verteilungspunkte fungieren, müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Über Verteilungspunkte

Ein Gerät, auf dem der Administrationsagent installiert ist, kann als Verteilungspunkt verwendet werden. In diesem Modus kann der Administrationsagent Updates verteilen, die entweder vom Administrationsserver oder von den Kaspersky Servern abgerufen werden können. Konfigurieren Sie im letzteren Fall den Update-Download für einen Verteilungspunkt.

Die Bereitstellung von Verteilungspunkten in einem Unternehmensnetzwerk hat die folgenden Ziele:

- Entlastung des Administrationsservers.

- Optimieren des Datenverkehrs.

- Dem Administrationsserver wird Zugriff auf Geräte gewährt, die sich an schwer erreichbaren Standorten des Unternehmensnetzwerks befinden. Wenn sich ein Verteilungspunkts in einem Netzwerk, hinter einer NAT befindet (in Bezug auf den Administrationsserver), kann der Administrationsserver Folgendes tun:
  - Nachrichten an Geräte in IPv4- oder IPv6-Netzwerken über UDP versenden
  - Das IPv4- oder IPv6-Netzwerk abfragen
  - Erstmalige Bereitstellung ausführen
  - Als Push-Server fungieren

Ein Verteilungspunkt wird für eine Administrationsgruppe bestimmt. In diesem Fall umfasst der Bereich des Verteilungspunktes alle Geräte, die sich in der Administrationsgruppe und allen ihren Untergruppen befinden. Dabei muss sich das Gerät, das als Verteilungspunkt fungiert, nicht in der Administrationsgruppe befinden, welcher es zugewiesen wurde.

Sie können einen Verteilungspunkt als Verbindungs-Gateway nutzen. Die Geräte, die zum Bereich des Verteilungspunktes gehören, werden in diesem Fall nicht direkt, sondern über ein Gateway mit dem Administrationsserver verbunden. Dieser Modus kann in Szenarien nützlich sein, bei denen keine direkte Verbindung zwischen dem Administrationsserver und den verwalteten Geräten möglich ist.

Wenn Sie ein Linux-basiertes Gerät als Verteilungspunkt verwenden, wird es dringend empfohlen, die Anzahl der Datei-Deskriptoren für den klnagent-Dienst zu erhöhen. Dies ist notwendig, da der Gültigkeitsbereich des Verteilungspunkts so viele Geräte umfassen kann, dass die standardmäßige maximale Anzahl von Dateien, die geöffnet werden können, nicht ausreicht.

Typische Konfiguration von Verteilungspunkten: Einzelbüro

In einer typischen Einzelbüro-Konfiguration befinden sich alle Geräte im Netzwerk des Unternehmens und können einander "sehen". Das Netzwerk des Unternehmens kann aus mehreren ausgewählten Teilen (der Netzwerke oder der Netzwerksegmente) bestehen, die über enge Kanäle verbunden sind.

Es sind die folgenden Methoden für den Aufbau der Struktur der Administrationsgruppen möglich:

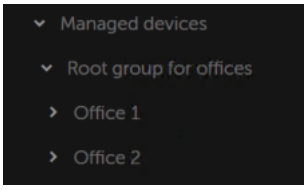
- Aufbau der Struktur der Administrationsgruppen unter Berücksichtigung der Netztopologie. Die Struktur der Administrationsgruppen muss die Netztopologie nicht unbedingt genau widerspiegeln. Es ist ausreichend, wenn den einzelnen Teilen des Netzwerkes bestimmte Administrationsgruppen entsprechen. Die Verteilungspunkte können automatisch bestimmt oder manuell zugewiesen werden.

- Aufbau der Struktur der Administrationsgruppen, in der die Netztopologie nicht widergespiegelt wird. In diesem Fall müssen Sie die automatische Bestimmung der Verteilungspunkte deaktivieren und dann für die Stammadministrationsgruppe in jedem ausgewählten Teil des Netzwerkes ein oder mehrere Geräte als Verteilungspunkte bestimmen, beispielsweise für die Gruppe **Verwaltete Geräte**. Alle Verteilungspunkte befinden sich dann auf einer Ebene und haben den identischen Gültigkeitsbereich, der alle Geräte im Netzwerk des Unternehmens umfasst. Jeder Administrationsagent wird in diesem Fall mit dem Verteilungspunkt verbunden, zu dem die Route am kürzesten ist. Die Route zum Verteilungspunkt kann mithilfe des Tools "tracert" bestimmt werden.

Typische Konfiguration von Verteilungspunkten: Mehrere kleine, eigenständige Büros

Diese typische Konfiguration entspricht einer Menge kleiner Remote-Büros, die eventuell durch das Internet mit dem Hauptbüro verbunden sind. Jedes der Remote-Büros befindet sich hinter einer NAT. Das bedeutet, dass ein Remote-Büro nicht mit einem anderen verbunden werden kann und die Büros voneinander isoliert sind.

Diese Konfiguration muss in der Struktur der Administrationsgruppen widergespiegelt werden: für jedes Remote-Büro muss eine separate Administrationsgruppe erstellt werden (entspr. Gruppen **Büro 1**, **Büro 2** auf der nachfolgenden Abbildung).



Die Remote-Büros werden in der Struktur der Administrationsgruppen abgebildet.

Für jede Administrationsgruppe, die einem Büro entspricht, müssen ein oder mehrere Verteilungspunkte festgelegt werden. Als Verteilungspunkte müssen Geräte des Remote-Büros bestimmt werden, die genug freien Platz auf dem Datenträger haben. Die Geräte, die sich beispielsweise in der Gruppe **Büro 1** befinden, wenden sich an die Verteilungspunkte, die für die Administrationsgruppe **Büro 1** bestimmt wurden.

Wenn einige Benutzer samt ihren Laptops physisch zwischen Büros wechseln, müssen in jedem Remote-Büro zusätzlich zu den oben erwähnten Verteilungspunkten zwei oder mehrere Geräte ausgewählt und als Verteilungspunkte für die Administrationsgruppe der obersten Ebene bestimmt werden (Gruppe **Stammgruppe für die Büros** in der obigen Abbildung).

Beispiel: Es gibt einen Laptop, der sich in der Administrationsgruppe **Büro 1** befindet, aber physisch in ein Büro gebracht wird, das der Gruppe **Büro 2** entspricht. Nach dem Ortswechsel versucht der Administrationsagent auf dem Laptop, sich an die Verteilungspunkte zu wenden, die zur Gruppe **Büro 1** gehören. Diese Verteilungspunkte erweisen sich allerdings als nicht verfügbar. Dann beginnt der Administrationsagent, sich an die Verteilungspunkte zu wenden, die für die Gruppe **Stammgruppe für die Büros** bestimmt wurden. Da die Remote-Büros voneinander isoliert sind, werden von allen Verteilungspunkten, die für die Administrationsgruppe **Stammgruppe für die Büros** bestimmt wurden, nur die Zugriffe des Administrationsagenten auf die Verteilungspunkte erfolgreich sein, die für die Gruppe **Büro 2** bestimmt wurden. Das bedeutet, dass der Laptop zwar in der Administrationsgruppe bleibt, die dem ursprünglichen Büro entspricht, aber die Verteilungspunkte jenes Büros verwendet, in dem er sich in diesen Moment physisch befindet.

Anzahl und Konfiguration der Verteilungspunkte bestimmen

Je mehr Client-Geräte ein Netzwerk enthält, desto mehr Verteilungspunkte sind erforderlich. Es wird empfohlen, die automatische Zuweisung von Verteilungspunkten nicht zu deaktivieren. Bei aktivierter automatischer Zuweisung der Verteilungspunkte weist der Administrationsserver bei einer großen Anzahl an Client-Geräten automatisch Verteilungspunkte zu und bestimmt ihre Konfiguration.

Verwendung exklusiv zugewiesener Verteilungspunkte

Wenn Sie planen, als Verteilungspunkte eine Reihe von bestimmten Geräten zu verwenden (d. h., exklusiv zugewiesene Server), so können Sie auf die automatische Zuweisung der Verteilungspunkte verzichten. Überzeugen Sie sich in diesem Fall davon, dass die Geräte, die Sie zu Verteilungspunkten bestimmen möchten, über ausreichend freien Speicherplatz auf dem Datenträger verfügen, nicht regelmäßig abgeschaltet werden und dass auf ihnen der Ruhezustand deaktiviert ist.

Anzahl der exklusiv zugewiesenen Verteilungspunkte in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, ein einzelnes Netzwerksegment enthält

Anzahl der Client-Geräte in dem Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 300	0 (Es müssen keine Verteilungspunkte bestimmt werden)
Über 300	Akzeptabel: (N/10.000 +1), empfohlen: (N/5000+2), wobei N die Anzahl an Geräten im Netzwerk ist

Anzahl der exklusiv zugewiesenen Verteilungspunkte in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, mehrere Netzwerksegmente enthält

Anzahl der Client-Geräte pro Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 10	0 (Es müssen keine Verteilungspunkte bestimmt werden)
10–100	1
Über 100	Akzeptabel: (N/10.000 +1), empfohlen: (N/5000+2), wobei N die Anzahl an Geräten im Netzwerk ist

Verwendung von Standard-Client-Geräten (Workstations) als Verteilungspunkte

Wenn Sie planen, als Verteilungspunkte Standard-Client-Geräte (d. h., Workstations) zu verwenden, wird zur Vermeidung einer unnötigen Belastung des Administrationsservers empfohlen, die Verteilungspunkte auf folgende Weise zuzuweisen (s. nachfolgende Tabelle):

Anzahl der als Verteilungspunkte fungierenden Workstations in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, ein einzelnes Netzwerksegment enthält

Anzahl der Client-Geräte in dem Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 300	0 (Es müssen keine Verteilungspunkte bestimmt werden)
Über 300	(N/300 +1), wobei N die Anzahl an Geräten im Netzwerk ist, jedoch mindestens 3 Verteilungspunkte

Anzahl der als Verteilungspunkte fungierenden Workstations in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, mehrere Netzwerksegmente enthält

Anzahl der Client-Geräte pro Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 10	0 (Es müssen keine Verteilungspunkte bestimmt werden)
10–30	1
31–300	2
Über 300	(N/300 +1), wobei N die Anzahl an Geräten im Netzwerk ist, jedoch mindestens 3 Verteilungspunkte

Wenn ein Verteilungspunkt abgeschaltet (oder aus anderen Gründen nicht verfügbar) ist, können die verwalteten Geräte in seinem Bereich Updates vom Administrationsserver abrufen.

Verteilungspunkte automatisch zuweisen

Es wird empfohlen, die Verteilungspunkte automatisch zu bestimmen. In diesem Fall wählt Kaspersky Security Center Linux die Geräte, die zu Verteilungspunkten bestimmt werden, selbständig aus.

Geräte mit Microsoft Windows on Arm können nicht als Verteilungspunkte fungieren.

Um Verteilungspunkte automatisch zuzuweisen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

3. Wählen Sie die Option **Verteilungspunkte automatisch zuweisen** aus.

   Wenn die automatische Gerätezuweisung für Verteilungspunkte aktiviert ist, können die Einstellungen der Verteilungspunkte nicht manuell angepasst werden und die Liste der Verteilungspunkte kann nicht verändert werden.

4. Klicken Sie auf die Schaltfläche **Speichern**.

   Daraufhin beginnt der Administrationsserver damit, Verteilungspunkte automatisch zu bestimmen und ihre Einstellungen zu konfigurieren.

Verteilungspunkte manuell zuweisen

In Kaspersky Security Center Linux haben Sie die Möglichkeit, Geräte manuell zu Verteilungspunkten zu bestimmen.

Es wird empfohlen, die Verteilungspunkte automatisch zu bestimmen. In diesem Fall wählt Kaspersky Security Center Linux die Geräte, die zu Verteilungspunkten bestimmt werden, selbständig aus. Wenn Sie jedoch aus bestimmten Gründen auf die automatische Bestimmung der Verteilungspunkte verzichten möchten (beispielsweise wenn Sie speziell ausgewählte Server verwenden wollen), können Sie die Verteilungspunkte nach der Berechnung der Anzahl und Konfiguration der Verteilungspunkte manuell zuweisen.

Geräte, die als Verteilungspunkte fungieren, müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Geräte mit Microsoft Windows on Arm können nicht als Verteilungspunkte fungieren.

Um ein Gerät manuell zum Verteilungspunkt zu bestimmen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

3. Wählen Sie die Option **Verteilungspunkte manuell zuweisen** aus.

4. Klicken Sie auf die Schaltfläche **Zuweisen**.

5. Wählen Sie das Gerät aus, das Sie zu einem Verteilungspunkt machen möchten.

   Berücksichtigen Sie bei der Auswahl des Geräts die Besonderheiten des Verteilungspunkts und die Anforderungen an das Gerät, das die Rolle des Verteilungspunkts übernehmen soll.

6. Wählen Sie die Administrationsgruppe aus, die zum Gültigkeitsbereich des ausgewählten Verteilungspunkts gehören soll.

7. Klicken Sie auf die Schaltfläche **OK**.

   Der hinzugefügte Verteilungspunkt wird in der Liste der Verteilungspunkte im Abschnitt **Verteilungspunkte** angezeigt.

8. Klicken Sie den hinzugefügten Verteilungspunkt in der Liste an, um sein Eigenschaftenfenster zu öffnen.

9. Passen Sie im Eigenschaftenfenster die Einstellungen des Verteilungspunkts an:

   - Der Abschnitt **Allgemein** enthält die Einstellungen für die Interaktion des Verteilungspunkts mit den Client-Geräten.

     - **SSL-Port**

       Nummer des SSL-Ports, über den die geschützte Verbindung des Client-Geräts mit dem Verteilungspunkt über das SSL-Protokoll erfolgt.

       Standardmäßig ist die Portnummer 13000 festgelegt.

     - **Aktiviert**

       Wenn diese Option aktiviert ist, werden die Installationspakete automatisch mithilfe von IP-Multicasting an die Client-Geräte innerhalb einer Gruppe verteilt.

       IP-Multicasting erhöht die Dauer für die Installation einer Anwendung aus einem Installationspaket in eine Gruppe von Client-Geräten. Dagegen reduziert es die Installationsdauer, wenn Sie eine Anwendung auf einem einzelnen Client-Gerät installieren.

     - **Adresse für IP-Multicast**

       IP-Adresse, die für das Multicasting verwendet wird. Die IP-Adresse kann man im Bereich 224.0.0.0 – 239.255.255.255 festgelegt werden.

       Standardmäßig weist Kaspersky Security Center Linux automatisch eine eindeutige IP-Multicast-Adresse innerhalb des angegeben Bereichs zu.

     - **Portnummer für IP-Multicast**

       Portnummer für das IP-Multicasting.

       Standardmäßig wird Port 15001 verwendet. Wenn als Verteilungspunkt ein Gerät angegeben wurde, auf dem der Administrationsserver installiert ist, wird für die Verbindung mit dem SSL-Protokoll standardmäßig Port 13001 verwendet.

     - **Adresse des Verteilungspunkts für Remote-Geräte**

       Die Netzwerkadresse, über die Remote-Geräte eine Verbindung zum Verteilungspunkt herstellen.

- **Aktiviert**

  Aus den folgenden Quellen werden Updates an verwaltete Geräte verteilt:

  - Von diesen Verteilungspunkt, wenn diese Option aktiviert ist.
  - Von anderen Verteilungspunkten, dem Administrationsserver oder Kaspersky-Update-Servern, wenn diese Option deaktiviert ist.

  Wenn Sie zur Bereitstellung von Updates Verteilungspunkte verwenden, können Sie Datenverkehr sparen, da Sie die Anzahl der Downloads reduzieren. Außerdem können Sie den Administrationsserver entlasten und die Last auf die Verteilungspunkten verlegen. Um den Datenverkehr und die Last zu optimieren, können Sie die Anzahl der Verteilungspunkte für Ihr Netzwerk berechnen.

  Wenn Sie diese Option deaktivieren, kann sich die Anzahl der Update-Downloads und die Belastung des Administrationsservers erhöhen. Diese Option ist standardmäßig aktiviert.

- **Aktiviert**

  Aus den folgenden Quellen werden Installationspakete an verwaltete Geräte verteilt:

  - Von diesen Verteilungspunkt, wenn diese Option aktiviert ist.
  - Von anderen Verteilungspunkten, dem Administrationsserver oder Kaspersky-Update-Servern, wenn diese Option deaktiviert ist.

  Wenn Sie zur Bereitstellung von Installationspaketen Verteilungspunkte verwenden, können Sie Datenverkehr sparen, da Sie die Anzahl der Downloads reduzieren. Außerdem können Sie den Administrationsserver entlasten und die Last auf die Verteilungspunkten verlegen. Um den Datenverkehr und die Last zu optimieren, können Sie die Anzahl der Verteilungspunkte für Ihr Netzwerk berechnen.

  Wenn Sie diese Option deaktivieren, kann sich die Anzahl der Downloads von Installationspaketen und die Belastung des Administrationsservers erhöhen. Diese Option ist standardmäßig aktiviert.

- **Aktiviert**

  In Kaspersky Security Center Linux kann ein Verteilungspunkt als Push-Server für Geräte fungieren, die über das mobile Protokoll oder über den Administrationsagenten verwaltet werden. Ein Push-Server muss beispielsweise aktiviert sein, wenn Sie die erzwungene Synchronisierung von KasperskyOS-Geräten mit dem Administrationsserver verwenden möchten. Ein Push-Server besitzt denselben Umfang verwalteter Geräte wie der Verteilungspunkt, auf dem der Push-Server aktiviert ist. Wenn Sie mehrere Verteilungspunkte derselben Administrationsgruppe zugewiesen haben, können Sie den Push-Server auf jedem der Verteilungspunkte aktivieren. In diesem Fall verteilt der Administrationsserver die Last zwischen den Verteilungspunkten.

- **Port des Push-Servers**

  Die Portnummer des Push-Servers. Sie können die Nummer eines beliebigen unbelegten Ports angeben.

- Geben Sie im Abschnitt **Bereich** die Administrationsgruppen an, an die der Verteilungspunkt Updates verteilen soll.

- Im Abschnitt **Update-Quelle** können Sie eine Update-Quelle für den Verteilungspunkt auswählen:

  - **Update-Quelle**

    Wählen Sie eine Update-Quelle für den Verteilungspunkt aus:

    - Damit der Verteilungspunkt die Updates vom Administrationsserver erhält, wählen Sie **Vom Administrationsserver beziehen**.
    - Damit Verteilungspunkte Updates anhand einer Aufgabe beziehen können, wählen Sie **Aufgabe zum Update-Download verwenden** aus und geben Sie anschließend eine Aufgabe vom Typ *Download*

von Updates in die Datenverwaltung der Verteilungspunkte an:

- Wenn eine solche Aufgabe bereits auf dem Gerät vorhanden ist, wählen Sie die Aufgabe in der Liste aus.
- Wenn auf dem Gerät noch keine derartige Aufgabe vorhanden ist, klicken Sie auf den Link **Aufgabe erstellen**, um eine Aufgabe zu erstellen. Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

- **Diff-Dateien herunterladen**

  Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

  Diese Option ist standardmäßig aktiviert.

- Wenn Ihre Verteilungspunkte für die Verbindung mit dem Internet einen Proxyserver verwenden, können Sie im Unterabschnitt **Einstellungen für die Internetverbindung** die folgenden Einstellungen festlegen:

  - **Proxyserver verwenden**

    Wenn Sie das Kontrollkästchen aktivieren, können Sie in den Eingabefeldern die Verbindungseinstellungen zum Proxyserver angeben.

    Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

  - **Proxyserver-Adresse**

    Proxyserver-Adresse.

  - **Portnummer**

    Nummer des Ports, über den die Verbindung erfolgt.

  - **Proxyserver für lokale Adressen umgehen**

    Wenn die Option aktiviert ist, wird bei der Verbindung mit den Geräten im lokalen Netzwerk kein Proxyserver verwendet.

    Diese Option ist standardmäßig deaktiviert.

  - **Authentifizierung am Proxyserver**

    Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

    Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

  - **Benutzername**

    Benutzerkonto, unter dessen Namen die Verbindung mit dem Proxy-Server hergestellt wird.

  - **Kennwort**

    Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

- Im Abschnitt **KSN-Proxy** können Sie die Anwendung anpassen, um den Verteilungspunkt zum Weiterleiten von KSN-Anfragen von den verwalteten Geräten zu verwenden:

  - **KSN-Proxy auf dem Verteilungspunkt aktivieren**

    Der KSN-Proxy-Service wird auf dem Gerät ausgeführt, das als Verteilungspunkt verwendet wird. Verwenden Sie diese Funktion, um Datenverkehr im Netzwerk neu zu verteilen und zu optimieren.

    Der Verteilungspunkt sendet die KSN-Statistik, die in der Erklärung zu Kaspersky Security Network aufgeführt sind, an Kaspersky.

    Diese Option ist standardmäßig deaktiviert. Die Aktivierung dieser Option wird erst wirksam, wenn im Fenster mit den Eigenschaften des Administrationsservers die Optionen **Administrationsserver als Proxyserver verwenden** und **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** aktiviert sind.

    Sie können dem Knoten eines aktiv-passiven Clusters die Rolle als Verteilungspunkt zuweisen und den KSN-Proxyserver auf diesem Knoten aktivieren.

  - **KSN-Anfragen an den Administrationsserver weiterleiten**

    Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an den Administrationsserver weiter.

    Diese Option ist standardmäßig aktiviert.

  - **Direkt über das Internet auf KSN Cloud/KPSN zugreifen**

    Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an die KSN Cloud oder an KPSN weiter. KSN-Anfragen, die der Verteilungspunkt selbst generiert, werden ebenso direkt an KSN Cloud oder KPSN gesendet.

  - **Proxyserver-Einstellungen beim Verbinden mit KPSN ignorieren**

    Aktivieren Sie diese Option, wenn Sie die Proxyserver-Einstellungen in den Eigenschaften des Verteilungspunkts oder in der Richtlinie des Administrationsagenten angepasst haben, aber Ihre Netzwerkarchitektur eine direkte Verwendung von KPSN erfordert. Andernfalls können Anfragen von den verwalteten Apps KPSN nicht erreichen.

    Diese Option ist verfügbar, wenn Sie die Option **Direkt über das Internet auf KSN Cloud/KPSN zugreifen** auswählen.

  - **Port**

    Die Nummer des TCP-Ports, den die verwalteten Geräte verwenden werden, um eine Verbindung mit dem KSN-Proxyserver herzustellen. Standardmäßig wird Portnummer 13111 verwendet.

  - **UDP-Port verwenden**

    Wenn es erforderlich ist, dass sich die verwalteten Geräte über einen UDP-Port mit dem KSN-Proxyserver verbinden, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine UDP-Portnummer an. Diese Option ist standardmäßig aktiviert.

  - **UDP-Port**

    Die Nummer des UDP-Ports, den die verwalteten Geräte verwenden werden, um eine Verbindung mit dem KSN-Proxyserver herzustellen. Der standardmäßige UDP-Port für die Verbindung zum KSN-Proxyserver ist 15111.

- **HTTPS verwenden**

  Wenn es erforderlich ist, dass sich die verwalteten Geräte über einen HTTPS-Port mit dem KSN-Proxyserver verbinden, aktivieren Sie die Option **HTTPS-Port verwenden** und geben Sie im Feld **HTTPS über Port** eine Nummer an. Der standardmäßige HTTPS-Port für die Verbindung zum KSN-Proxyserver ist 17111.

- **HTTPS-Port**

  Die Nummer des HTTPS-Ports, den die verwalteten Geräte verwenden sollen, um eine Verbindung mit dem KSN-Proxyserver herzustellen. Der standardmäßige HTTPS-Port für die Verbindung zum KSN-Proxyserver ist 17111.

- Im Abschnitt **Verbindungs-Gateway** können Sie den Verteilungspunkt so konfigurieren, dass er als Gateway für die Verbindung zwischen den Instanzen des Administrationsagenten und dem Administrationsserver fungieren soll:

  - **Verbindungs-Gateway**

    Wenn aufgrund der Organisation Ihres Netzwerks keine direkte Verbindung zwischen dem Administrationsserver und den Administrationsagenten hergestellt werden kann, können Sie den Verteilungspunkt als Verbindungs-Gateway zwischen Administrationsserver und Administrationsagenten verwenden.

    Aktivieren Sie diese Option, wenn der Verteilungspunkt als Verbindungs-Gateway zwischen den Administrationsagenten und dem Administrationsserver fungieren soll. Diese Option ist standardmäßig deaktiviert.

  - **Verbindung zum Gateway ausgehend vom Administrationsserver herstellen (falls sich das Gateway in der DMZ befindet)**

    Wenn sich der Administrationsserver außerhalb der demilitarisierten Zone (DMZ) in einem lokalen Netzwerk befindet, können auf Remote-Geräten installierte Administrationsagenten keine Verbindung zum Administrationsserver herstellen. Sie können einen Verteilungspunkt als Verbindungs-Gateway mit Reverse Connectivity verwenden (der Administrationsserver stellt eine Verbindung zum Verteilungspunkt her).

    Aktivieren Sie diese Option, wenn Sie den Administrationsserver mit dem Verbindungs-Gateway in der DMZ verbinden müssen.

  - **Lokalen Port für Kaspersky Security Center Web Console öffnen**

    Aktivieren Sie diese Option, wenn Sie das Verbindungs-Gateway in der DMZ benötigen, um einen Port für die Web Console zu öffnen, der sich in der DMZ oder im Internet befindet. Geben Sie die Portnummer an, die für die Verbindung von der Web Console zum Verteilungspunkt verwendet wird. Standardmäßig wird Portnummer 13299 verwendet.

    Diese Option ist verfügbar, wenn Sie die Option **Verbindung zum Gateway ausgehend vom Administrationsserver herstellen (falls sich das Gateway in der DMZ befindet)** aktivieren.

  Wenn Sie mobile Geräte über den Verteilungspunkt, der als Verbindungs-Gateway fungiert, mit dem Administrationsserver verbinden, können Sie die folgenden Optionen aktivieren:

  - **Port für mobile Geräte öffnen (nur SSL-Authentifizierung des Administrationsservers)**

    Aktivieren Sie diese Option, wenn das Verbindungs-Gateway einen Port für mobile Geräte öffnen soll, und geben Sie die Portnummer an, die mobile Geräte für die Verbindung zum Verteilungspunkt verwenden. Standardmäßig wird Portnummer 13292 verwendet. Das mobile Gerät überprüft das Zertifikat des Administrationsservers. Beim Verbindungsaufbau wird nur der Administrationsserver authentifiziert.

- **Port für mobile Geräte öffnen (bidirektionale SSL-Authentifizierung)**

  Aktivieren Sie diese Option, wenn Sie ein Verbindungs-Gateway benötigen, um einen Port zu öffnen, der für die bidirektionale Authentifizierung des Administrationsservers und mobiler Geräte verwendet wird. Das mobile Gerät überprüft das Zertifikat des Administrationsservers und der Administrationsserver überprüft das Zertifikat des mobilen Geräts. Geben Sie die folgenden Parameter an:

  - Portnummer, die mobile Geräte für die Verbindung mit dem Verteilungspunkt verwenden. Standardmäßig wird Portnummer 13293 verwendet.

  - DNS-Domänennamen des Verbindungs-Gateways, die von mobilen Geräten verwendet werden. Trennen Sie Domänennamen durch Kommas. Die angegebenen Domänennamen werden in das Zertifikat des Verteilungspunkts aufgenommen. Wenn die von den mobilen Geräten verwendeten Domänennamen nicht mit dem allgemeinen Namen im Verteilungspunktzertifikat übereinstimmen, stellen die mobilen Geräte keine Verbindung zum Verteilungspunkt her.

    Standardmäßig entspricht der DNS-Domänenname dem FQDN-Namen des Verbindungsgateways.

  In beiden Fällen werden die Zertifikate nur während des Aufbaus der TLS-Sitzung auf dem Verteilungspunkt überprüft. Die Zertifikate werden nicht zur Prüfung durch den Administrationsserver weitergeleitet. Nachdem eine TLS-Sitzung mit dem mobilen Gerät hergestellt wurde, verwendet der Verteilungspunkt das Zertifikat des Administrationsservers, um einen Tunnel für die Synchronisierung zwischen dem mobilen Gerät und dem Administrationsserver herzustellen. Wenn Sie den Port für die bidirektionale SSL-Authentifizierung öffnen, kann das Zertifikat für mobile Geräte nur mithilfe eines Installationspakets verteilt werden.

- Konfigurieren der Windows-Netzwerkabfrage über den Windows-basierten Verteilungspunkt.

  - **Windows-Domänen**

    Sie können für Windows-Domänen die Gerätesuche erlauben und den Zeitplan für die Abfrage festlegen.

- Konfigurieren Sie die Abfrage des Domänencontrollers mittels eines Verteilungspunkts.

  - **Abfrage des Domänencontrollers**

    Sie können für Domänencontroller die Gerätesuche aktivieren.

    Nachdem Sie im Feld **Abfrage** die Taste auf **Aktiviert** gewechselt haben, können Sie Domänencontroller für die Abfrage auswählen und den Abfragezeitplan für diese festlegen.

    Wenn Sie einen Linux-Verteilungspunkt verwenden, klicken Sie im Abschnitt **Angegebene Domänen abfragen** auf **Hinzufügen** und geben Sie anschließend die Adresse und die Anmeldeinformationen des Domänencontrollers an. Außerdem können Sie den Typ der abzufragenden Domäne angeben: Active Directory oder Samba, FreeIPA, ALD Pro.

    Wenn Sie einen Windows-Verteilungspunkt verwenden, können Sie eine der folgenden Optionen auswählen:

    - **Aktuelle Domäne abfragen**

    - **Domänengesamtstruktur abfragen**

    - **Angegebene Domänen abfragen**

- Konfigurieren Sie die Abfrage von IP-Bereichen durch den Verteilungspunkt.

  - **IP-Bereiche abfragen**

    Sie können die Gerätesuche für IPv4-Bereiche und IPv6-Netzwerke aktivieren.

Wenn Sie die Option **Abfrage des Bereichs zulassen** aktivieren, können Sie zu untersuchende Bereiche hinzufügen und den Zeitplan für sie festlegen. Sie können IP-Bereich zur Liste der untersuchten Bereiche hinzufügen.

Wenn Sie die Option **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden** aktiviert haben, fragt der Verteilungspunkt das IPv6-Netzwerk automatisch unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) ab. In diesem Fall werden angegebene IP-Bereiche ignoriert, da der Verteilungspunkt das gesamte Netzwerk abfragt. Für Verteilungspunkte mit Linux ist die Option **Zeroconf zum Abfragen von IPv6-Netzwerken verwenden** verfügbar. Um die Zeroconf-IPv6-Abfrage verwenden zu können, müssen Sie das Tool "avahi-browse" auf dem Verteilungspunkt installieren.

- Geben Sie im Abschnitt **Erweitert** den Ordner an, den der Verteilungspunkt zum Speichern der zu verteilenden Daten verwenden soll.

  - **Standardordner verwenden**

    Bei Auswahl dieser Option wird zum Speichern der Ordner auf dem Verteilungspunkt verwendet, in dem der Administrationsagent installiert wurde.

  - **Benutzerdefinierten Ordner verwenden**

    Bei Auswahl dieser Option können Sie im unteren Feld den Pfad zum Ordner angeben. Dabei können Sie einen lokalen Ordner des Verteilungspunkts oder einen Ordner auf einem beliebigen, sich im Unternehmensnetzwerk befindlichen Remote-Gerät angeben.

    Das Benutzerkonto, unter dem der Administrationsagent auf dem Verteilungspunkt gestartet wird, muss über die Lese- und Schreibberechtigungen für den angegebenen Ordner verfügen.

10. Klicken Sie auf die Schaltfläche **OK**.

Daraufhin übernehmen die ausgewählten Geräte die Rolle des Verteilungspunkts.

Hinzufügen eines Verbindungs-Gateways als Verteilungspunkt innerhalb der DMZ

Wenn der Administrationsserver nicht zur demilitarisierten Zone (DMZ) gehört, können sich Administrationsagenten, die auf externen Geräten installiert wurden, nicht mit dem Administrationsserver verbinden. In diesem Fall können Sie einen Verteilungspunkt als Verbindungs-Gateway in die DMZ verwenden. Der Verteilungspunkt öffnet einen Port für den Administrationsserver, damit die Verbindung hergestellt werden kann. Der Administrationsserver stellt beim Starten eine Verbindung zum Verteilungspunkt her und trennt diese Verbindung während seines Betriebs nicht.

Wenn Sie außerhalb des Synchronisierungszeitraums zwischen Administrationsagent und Administrationsserver eine Verbindung zwischen dem Administrationsagenten und Ihren verwalteten Geräten herstellen müssen, ist es erforderlich, einen Push-Server zu aktivieren und den Port 13295 auf der Seite des Verteilungspunkts zu öffnen.

Es wird empfohlen, ein speziell dafür vorgesehenes Gerät als Verbindungsgateway zu verwenden. Weitere Informationen zur maximalen Anzahl der Client-Geräte (einschließlich mobiler Geräte) finden Sie im Skalierungshandbuch.

Statt selbst eine Verbindung zum Administrationsserver herzustellen, wartet ein Verbindungs-Gateway auf eine Verbindung vom Administrationsserver. Das bedeutet, dass das Gerät mit dem Verbindungs-Gateway in der DMZ direkt nach der Installation des Verbindungs-Gateways vom Administrationsserver nicht unter den verwalteten Geräten angezeigt wird. Es ist daher eine spezielle Vorgehensweise notwendig, um sicherzustellen, dass der Administrationsserver eine Verbindung zum Verbindungs-Gateway initiiert.

Um ein Gerät mit einem Verbindungs-Gateway als Verteilungspunkt hinzuzufügen:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

3. Wählen Sie die Option **Verteilungspunkte manuell zuweisen** aus.

4. Klicken Sie in der Werkzeugleiste auf die **Zuweisen** Importieren.

5. Führen Sie im neu geöffneten rechten Bereich Folgendes aus:

   a. Wählen Sie die Option **Verbindungs-Gateway in der DMZ anhand seiner Adresse verwenden**.

   b. Geben Sie im Feld **Adresse des Verbindungs-Gateways** die IP-Adresse oder den DNS-Namen des Geräts an.

   c. Klicken Sie auf die Schaltfläche **Zuweisen**.

   d. Der Bereich schließt sich und der Verteilungspunkt wird mit dem Namen **Temporärer Eintrag für das Verbindungs-Gateway** angezeigt.

6. Klicken Sie auf die Schaltfläche **Speichern**.

   Der Administrationsserver versucht, sich mit dem Verbindungs-Gateway über die von Ihnen angegebene Adresse zu verbinden. Ist dies erfolgreich, wird der Name des Eintrags in den Namen des Geräts mit dem Verbindungs-Gateway geändert. Dieser Vorgang kann bis zu 5 Minuten dauern.

Wenn Sie durch Anklicken von **Temporärer Eintrag für das Verbindungs-Gateway** die Eigenschaften des Verteilungspunkts öffnen, sind dort alle Optionen inaktiv. Sie können nur die Registerkarte "Allgemein" anzeigen, die den Namen des Verteilungspunkts enthält. Standardmäßig ist die Portnummer (13000) festgelegt. Sie können den Verteilungspunkt erst konfigurieren, wenn sich der Administrationsserver mit ihm verbunden hat. Während der Konvertierung des temporären Eintrags für den Verbindungs-Gateway in einen benannten Eintrag, wird das Verbindungs-Gateway auch in der Gruppe Nicht zugeordnete Geräte angezeigt.

So fügen Sie einem zuvor konfigurierten Netzwerk ein Verbindungs-Gateway hinzu:

1. Installieren Sie Administrationsagenten Verbindungs-Gateway-Modus.

2. Installieren Sie den Administrationsagenten auf den Geräten erneut, die Sie mit dem neu hinzugefügten Verbindungs-Gateway verbinden möchten.

Liste mit Verteilungspunkten für eine Administrationsgruppe bearbeiten

Sie können eine Liste mit Verteilungspunkten anzeigen, die einer bestimmten Administrationsgruppe zugewiesen wurden, und Verteilungspunkte zu dieser Liste hinzufügen oder daraus löschen.

Um die Liste mit Verteilungspunkten, die einer Administrationsgruppe zugewiesen wurden, zu bearbeiten, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.
2. Eine Administrationsgruppe, für die Sie die zugewiesenen Verteilungspunkte anzeigen wollen, wählen Sie aus, indem Sie im oberen Bereich der Seite auf **Hierarchie anzeigen** klicken und anschließend im neuen Fenster den Namen der erforderlichen Gruppe anklicken.

   Dadurch wird der Menüpunkt **Verteilungspunkte** aktiviert.

   Der Pfad zur ausgewählten Gruppe wird im oben Bereich der Seite angezeigt. Bei Bedarf können Sie innerhalb dieses Pfades auf einen Link mit dem Namen der Administrationsgruppe klicken, um zu dieser Gruppe zu gelangen. Der letzte Link im Pfad ist standardmäßig inaktiv.
3. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Verteilungspunkte**.
4. Um der Administrationsgruppe neue Verteilungspunkte hinzuzufügen, klicken Sie auf die Schaltfläche **Zuweisen**.
5. Um die zugewiesenen Verteilungspunkte zu entfernen, wählen Sie Geräte aus der Liste aus und klicken Sie auf die Schaltfläche **Zuweisen aufheben**.

Je nach Ihren Änderungen werden neue Verteilungspunkte zur Liste hinzugefügt oder bestehende Verteilungspunkte daraus entfernt.

Push-Server aktivieren

In Kaspersky Security Center Linux kann ein Verteilungspunkt als Push-Server für Geräte fungieren, die über das mobile Protokoll oder über den Administrationsagenten verwaltet werden. Ein Push-Server muss beispielsweise aktiviert sein, wenn Sie die erzwungene Synchronisierung von KasperskyOS-Geräten mit dem Administrationsserver verwenden möchten. Ein Push-Server besitzt denselben Umfang verwalteter Geräte wie der Verteilungspunkt, auf dem der Push-Server aktiviert ist. Wenn Sie mehrere Verteilungspunkte derselben Administrationsgruppe zugewiesen haben, können Sie den Push-Server auf jedem der Verteilungspunkte aktivieren. In diesem Fall verteilt der Administrationsserver die Last zwischen den Verteilungspunkten.

Möglicherweise möchten Sie Verteilungspunkte als Push-Server verwenden, um sicherzustellen, dass eine kontinuierliche Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver besteht. Für einige Vorgänge ist eine durchgängige Verbindung erforderlich, z. B. das Starten und Stoppen lokaler Aufgaben, das Empfangen von Statistiken für eine verwaltete Anwendung oder die Herstellung eines Tunnels. Wenn Sie einen Verteilungspunkt als Push-Server verwenden, müssen Sie weder die Option **Verbindung zum Administrationsserver nicht trennen** auf verwalteten Geräten verwenden, noch Pakete an den UDP-Port des Administrationsagenten senden.

Ein Push-Server unterstützt die Last von bis zu 50.000 gleichzeitigen Verbindungen.

So aktivieren Sie Push-Server auf einem Verteilungspunkt:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.
3. Klicken Sie auf den Namen des Verteilungspunkts, auf dem Sie den Push-Server aktivieren möchten.

   Das Eigenschaftenfenster des Verteilungspunkts wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** die Option **Aktiviert**.

5. Geben Sie im Feld **Port des Push-Servers** die Portnummer ein. Sie können die Nummer eines beliebigen unbelegten Ports angeben.

6. Geben Sie im Feld **Remote-Host-Adresse** die IP-Adresse oder den Namen des Geräts mit dem Verteilungspunkt an.

7. Klicken Sie auf die Schaltfläche **OK**.

Der Push-Server ist auf dem ausgewählten Verteilungspunkt aktiviert.

Anzahl der Datei-Deskriptoren für den klnagent-Dienst erhöhen

Wenn der Gültigkeitsbereich eines Linux-basierten Verteilungspunkts viele Geräte umfasst, ist die standardmäßige Beschränkung der Dateien, die geöffnet werden können (Datei-Deskriptoren), möglicherweise nicht ausreichend. Um dies zu vermeiden, können Sie das Limit der Datei-Deskriptoren für den klnagent-Dienst erhöhen.

So erhöhen Sie die Anzahl der Datei-Deskriptoren für den klnagent-Dienst:

1. Führen Sie auf dem Linux-basierten Gerät, das als Verteilungspunkt agiert, den folgenden Befehl aus:

   ```
   systemctl edit klnagent64.service
   ```

2. Geben Sie die harte und weiche Obergrenze der Dateideskriptoren im Parameter `LimitNOFILE` des Abschnitts `[Service]` an:

   `LimitNOFILE=<soft resource limit>:<hard resource limit>`

   Beispiel: `LimitNOFILE=32768:131072`. Beachten Sie, dass die flexible Beschränkung der Datei-Deskriptoren kleiner oder gleich der festen Beschränkung sein muss.

3. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die Parameter korrekt angegeben wurden:

   ```
   systemd-analyze verify klnagent64.service
   ```

   Bei ungültigen Parameterangaben kann dieser Befehl einen der folgenden Fehler ausgeben:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Wenn dieser Fehler auftritt, sind in der Zeile `LimitNOFILE` falsche Zeichen angegeben. Überprüfen und korrigieren Sie die eingegebene Zeile.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Wenn dieser Fehler auftritt, liegt die flexible Beschränkung der eingegebenen Datei-Deskriptoren über der festen Beschränkung. Überprüfen Sie die eingegebene Zeile und stellen Sie sicher, dass die flexible Beschränkung der Datei-Deskriptoren kleiner oder gleich der festen Beschränkung ist.

4. Führen Sie den folgenden Befehl aus, um den Prozess "systemd" neu zu laden:

   ```
   systemctl daemon-reload
   ```

5. Führen Sie den folgenden Befehl aus, um den Dienst des Administrationsagenten neu zu starten:

   ```
   systemctl restart klnagent
   ```

6. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die angegebenen Parameter korrekt angewendet werden:

   ```
   less /proc/<Prozess-ID von nagent>/limits
   ```

   wobei <Prozess-ID von nagent> der Prozess-ID des Administrationsagenten entspricht. Um die Prozess-ID zu erfahren, können Sie den folgenden Befehl ausführen:

   ```
   ps -ax | grep klnagent
   ```

Die Anzahl der Dateien, die geöffnet werden können, für den Linux-basierten Verteilungspunkt wurde erhöht.

Über die Varianten für den Gerätestatus

Kaspersky Security Center Linux weist jedem verwalteten Gerät einen Status zu. Der jeweilige Status hängt davon ab, ob die vom Benutzer definierten Bedingungen erfüllt sind. Wenn Kaspersky Security Center Linux einem Gerät einen Status zuweist, wird für bestimmte Bedingungen das Sichtbarkeits-Flag des Gerätes im Netzwerk berücksichtigt (siehe folgende Tabelle). Beispiel: Wenn einem verwalteten Gerät der Status *Kritisch* zugewiesen wurde, da die Bedingung *Die Datenbanken sind veraltet* erfüllt ist und für das Gerät später das Sichtbarkeits-Flag gesetzt wurde, erhält das Gerät den Status *OK*. Wenn Kaspersky Security Center Linux ein Gerät innerhalb von zwei Stunden nicht im Netzwerk findet, wird das Sichtbarkeits-Flag des Gerätes auf *Nicht sichtbar* gesetzt.

Es gibt folgende Statusvarianten:

- *Kritisch* oder *Kritisch/Sichtbar*
- *Warnung* oder *Warnung/Sichtbar*
- *OK* oder *OK/Sichtbar*

Die folgende Tabelle enthält die erforderlichen Standardbedingungen, nach denen einem Gerät der Status *Kritisch* oder *Warnung* zugewiesen wird, sowie alle möglichen Werte.

Bedingungen für das Zuweisen der Status an das Gerät

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Sicherheitsanwendung ist nicht installiert	Auf dem Gerät ist der Administrationsagent installiert, aber es wurde keine Sicherheitsanwendung installiert.	• Umschalter aktiviert. • Umschalter deaktiviert.
Zu viele Viren gefunden	Auf dem Gerät wurden als Ergebnis der Ausführung einer Aufgabe zur Virensuche (beispielsweise der Aufgabe zur Schadsoftware-Untersuchung) mehrere Viren gefunden, und die Anzahl der gefundenen Viren übersteigt den angegebenen Wert.	Über 0.
Die Stufe des Echtzeitschutzes unterscheidet sich von der Stufe, die der Administrator festgelegt hat	Das Gerät ist im Netzwerk sichtbar, aber die Stufe des Echtzeitschutzes unterscheidet sich von der Stufe, die vom Administrator (in der Bedingung) für den Gerätestatus eingestellt wurde.	• Beendet. • Angehalten. • Wird ausgeführt.
Die letzte Schadsoftware-Untersuchung liegt lange zurück	Das Gerät ist im Netzwerk sichtbar und es wurde eine Sicherheitsanwendung auf dem Gerät installiert, aber es wurde weder die Aufgabe zur *Schadsoftware-Untersuchung*, noch die Aufgabe zur lokalen Untersuchung innerhalb des angegebenen Zeitintervalls ausgeführt. Die Bedingung gilt nur für Geräte, die vor mehr als sieben Tagen zur Administrationsserver-Datenbank hinzugefügt wurden.	Über 1 Tag.
Die Datenbanken sind veraltet	Das Gerät ist im Netzwerk sichtbar und eine Sicherheitsanwendung wurde auf dem Gerät installiert, aber die Antiviren-Datenbanken wurden auf diesem Gerät nicht innerhalb des angegebenen Zeitintervalls aktualisiert. Die Bedingung gilt nur für Geräte, die vor mehr als einem Tag zur Administrationsserver-Datenbank hinzugefügt wurden.	Über 1 Tag.

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Die letzte Verbindung liegt lange zurück	Der Administrationsagent ist auf dem Gerät installiert, es wurde allerdings nicht innerhalb des angegebenen Zeitintervalls mit dem Administrationsserver verbunden, da es deaktiviert ist.	Über 1 Tag.
Aktive Bedrohungen wurden erkannt	Die Anzahl der unbearbeiteten Objekte im Ordner **Aktive Bedrohungen** übersteigt den angegebenen Wert.	Über 0 Elemente.
Neustart erforderlich seit	Das Gerät ist im Netzwerk sichtbar, aber eine Anwendung erfordert einen Neustart des Geräts. Der Zeitpunkt der Anfrage liegt länger zurück, als im Zeitintervall angegeben.	Über 0 Minuten.
Grund des Neustarts	Das Gerät ist im Netzwerk sichtbar, aber eine Anwendung erfordert aus einem der ausgewählten Gründe einen Neustart des Geräts.	• Unbekannter Ursache • Anwendung wird erst nach Neustart ausgeführt • Um das Update abzuschließen, ist ein Neustart erforderlich; die Anwendung ist jedoch funktionsfähig • Zum Start des Updates ist ein Neustart erforderlich • Zum Abschließen der Untersuchung oder Desinfektion ist ein Neustart erforderlich • Um die Remote-Installation bzw. -Deinstallation abzuschließen, ist ein Neustart erforderlich • Abschließen der Datenverschlüsselung auf der Festplatte
Es sind inkompatible Anwendungen installiert	Das Gerät ist im Netzwerk sichtbar, aber infolge der Inventarisierung der Software durch den Administrationsagenten wurden auf dem Gerät inkompatible Anwendungen gefunden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Es wurden Schwachstellen in Programmen erkannt	Das Gerät ist im Netzwerk sichtbar und der Administrationsagent ist auf dem Gerät installiert, aber die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* hat in den Programmen auf dem Gerät Schwachstellen mit der angegebenen Signifikanz gefunden.	• Kritisch. • Hoch. • Normal. • Ignorieren, wenn die Schwachstelle nicht geschlossen werden kann. • Ignorieren, wenn das Update für die Installation bestimmt wurde.
Lizenz abgelaufen	Das Gerät ist im Netzwerk sichtbar, aber die Lizenz ist abgelaufen.	• Umschalter deaktiviert. • Umschalter aktiviert.
Die Lizenz läuft bald ab	Das Gerät ist im Netzwerk sichtbar, aber die Lizenz auf dem Gerät läuft in weniger als der angegebenen Anzahl an Tagen ab.	Über 0 Tage.

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Die letzte Suche nach Windows-Updates liegt lange zurück	Das Gerät ist im Netzwerk sichtbar, aber die Aufgabe *Finden von Schwachstellen und erforderlichen Updates* wurde nicht innerhalb des angegebenen Zeitintervalls ausgeführt.	Über 1 Tag.
Ungültiger Verschlüsselungsstatus	Der Administrationsagent ist auf dem Gerät installiert, aber das Ergebnis der Verschlüsselung des Geräts entspricht dem angegebenen Wert.	• Entspricht nicht der Richtlinie aufgrund der Ablehnung durch den Benutzer (nur für externe Geräte). • Entspricht nicht der Richtlinie wegen eines Fehlers. • Bei der Übernahme der Richtlinie – Neustart erforderlich. • Es wurde keine Verschlüsselungsrichtlinie festgelegt. • Nicht unterstützt. • Bei der Übernahme der Richtlinie.
Die Einstellungen des mobilen Geräts entsprechen nicht der Richtlinie	Die Einstellungen des mobilen Geräts unterscheiden sich von den in der Richtlinie von Kaspersky Endpoint Security für Android festgelegten Einstellungen beim Ausführen der Untersuchung der Übereinstimmungsregeln.	• Umschalter deaktiviert. • Umschalter aktiviert.
Es wurden unbearbeitete Sicherheitsprobleme erkannt	Auf dem Gerät sind unbearbeitete Sicherheitsvorfälle vorhanden. Sicherheitsvorfälle können sowohl automatisch mithilfe von auf dem Client-Gerät installierten verwalteten Kaspersky-Anwendungen als auch manuell durch den Administrator erstellt werden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Gerätestatus wird durch Anwendung bestimmt	Der Gerätestatus wird von der verwalteten Anwendung bestimmt. Verwaltete Geräte können einen Status besitzen, der von den verwalteten Anwendungen unabhängig von den Einstellungen von Kaspersky Security Center Linux bestimmt wird. Wenn der Status zu einem der Werte zurückkehrt, die durch Kaspersky Security Center Linux bestimmt werden, weist der Administrationsserver einem verwalteten Gerät den kritischsten Status zu, der von der verwalteten Anwendung zurückgegeben und vom Administrationsserver zugewiesen wurde. Statuswerte, die von verwalteten Anwendungen bestimmt werden, besitzen Beschreibungen, die ebenfalls von den verwalteten Anwendungen stammen. Sie können diese Beschreibungen in der Liste der verwalteten Geräte in der Spalte **Statusbeschreibung**.	• Umschalter ist deaktiviert. • Umschalter ist aktiviert.
Kein Platz auf dem Datenträger des Geräts	Der freie Speicherplatz auf dem Datenträger ist kleiner als der angegebene Wert oder das Gerät konnte nicht mit dem Administrationsserver synchronisiert werden. Der Status *Kritisch* oder *Warnung* wird in den Status *OK* geändert, wenn das Gerät erfolgreich mit dem Administrationsserver synchronisiert wird und der freie Speicherplatz auf dem Gerät dem angegebenen Wert entspricht oder diesen überschreitet.	Über 0 MB.
Das Gerät wird nicht mehr verwaltet	Bei der Gerätesuche ist das Gerät im Netzwerk sichtbar, aber es sind mehr als drei Synchronisierungsversuche mit dem Administrationsserver fehlgeschlagen.	• Umschalter deaktiviert. • Umschalter aktiviert.
Der Schutz ist deaktiviert	Das Gerät ist im Netzwerk sichtbar, aber die Sicherheitsanwendung auf dem Gerät ist länger deaktiviert, als im Zeitintervall angegeben. In diesem Fall lautet der Status der Sicherheitsanwendung *Angehalten* oder *Fehler* und unterscheidet sich von den folgenden Statuswerten *Wird gestartet*, *Wird ausgeführt* oder *Wird angehalten*.	Über 0 Minuten.
Die Sicherheitsanwendung wurde nicht gestartet	Das Gerät ist im Netzwerk sichtbar und eine Sicherheitsanwendung ist auf dem Gerät installiert, wurde aber nicht gestartet.	• Umschalter deaktiviert. • Umschalter aktiviert.

Kaspersky Security Center Linux ermöglicht es, den Status eines Gerätes in einer Administrationsgruppe unter bestimmten Bedingungen automatisch zu ändern. Bei Erfüllung der festgelegten Bedingungen wird dem Client-Gerät einer der folgenden Statuswerte verliehen: *Kritisch* oder *Warnung*. Sind die festgelegten Bedingungen nicht erfüllt, so erhält das Client-Gerät den Status *OK*.

Verschiedenen Werten einer einzelnen Bedingung können verschiedene Statusvarianten entsprechen. Beispiele: Wenn die Bedingung **Die Datenbanken sind veraltet** den Wert **Über 3 Tage** besitzt, erhält das Client-Gerät standardmäßig den Status *Warnung* und für den Wert **Über 7 Tage** wird ihm der Status *Kritisch* zugewiesen.

Wenn Sie ein Upgrade für Kaspersky Security Center Linux durchführen und es von einer früheren Version aktualisieren, bleiben die Werte der Bedingung **Die Datenbanken sind veraltet**, bei denen dem Gerät der Status *Warnung* oder *Kritisch* zugewiesen wird, identisch.

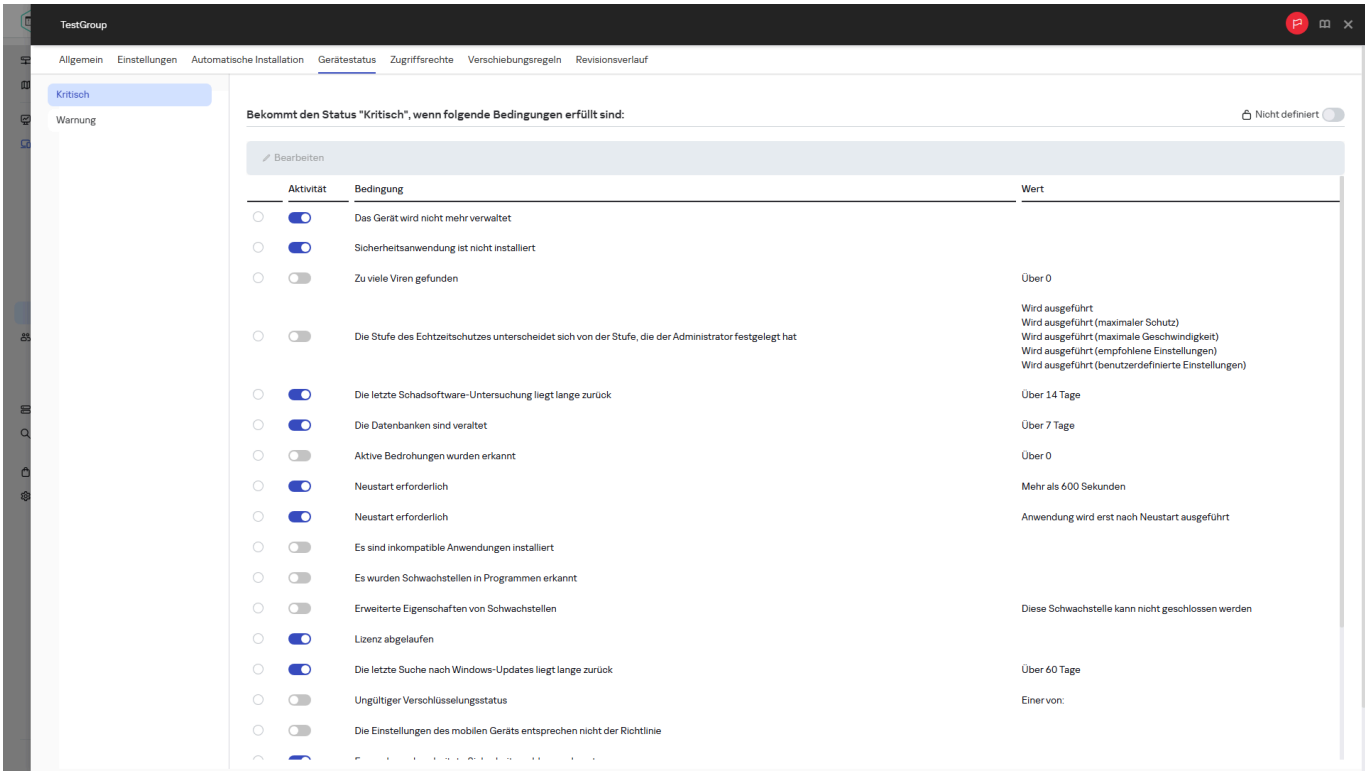
Wechsel der Statuswerte von Geräten konfigurieren

Sie können die Bedingungen ändern, um einem Gerät den Status *Kritisch* oder *Warnung* zuzuweisen.

Um die Änderungen des Gerätestatus auf Kritisch zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Gruppenhierarchie**.
2. Wechseln Sie auf eine der folgenden Arten zu den Eigenschaften der Administrationsgruppe, für welche Sie den Gerätestatus ändern möchten:
   - Klicken Sie auf den Namen der Administrationsgruppe.
   - Klicken Sie im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**. Bewegen Sie im neuen Navigationsbereich den Mauszeiger über den Namen der gewünschten Gruppe und klicken Sie anschließend auf das Einstellungssymbol (⚙).

   Das Eigenschaftenfenster der übergeordneten Administrationsgruppe wird geöffnet.
3. Klicken Sie im Eigenschaftsfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Kritisch** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Bekommt den Status "Kritisch" zugewiesen, wenn folgende Bedingungen erfüllt sind** die Bedingung zum Umschalten eines Geräts in den Status *Kritisch*.



Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.
8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.
   Es können nicht für alle Bedingungen Werte festgelegt werden.
9. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Kritisch*.

Um die Änderungen des Gerätestatus auf Warnung zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Gruppenhierarchie**.
2. Klicken Sie in der angezeigten Liste der Gruppen auf den Link mit dem Namen der Gruppe, für die Sie den Wechsel der Gerätestatus ändern möchten.
3. Klicken Sie im daraufhin geöffneten Eigenschaftenfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Warnung** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Bekommt den Status "Warnung" zugewiesen, wenn folgende Bedingungen erfüllt sind** die Bedingung zum Umschalten eines Geräts in den Status *Warnung*.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.
8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.
   Es können nicht für alle Bedingungen Werte festgelegt werden.
9. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Warnung*.

Geräteauswahlen

Geräteauswahlen sind ein Instrument zum Filtern von Geräten nach festgelegten Bedingungen. Sie können Geräteauswahlen verwenden, um mehrere Geräte zu verwalten: beispielsweise, um einen Bericht über nur diese Geräte anzuzeigen, oder um alle diese Geräte in eine andere Gruppe zu verschieben.

Kaspersky Security Center Linux bietet eine große Zahl an *vordefinierten Auswahlen* an (z. B. **Geräte mit dem Status "Kritisch"**, **Der Schutz ist deaktiviert**, **Aktive Bedrohungen wurden erkannt**). Vordefinierte Auswahlen können nicht gelöscht werden. Sie können auch zusätzliche *benutzerdefinierte Auswahlen* erstellen und konfigurieren.

In benutzerdefinierten Auswahlen können Sie den Suchbereich festlegen und alle Geräte, verwaltete Geräte oder nicht zugeordnete Geräte auswählen. Sucheinstellungen werden in den Bedingungen festgelegt. In der Geräteauswahl können Sie mehrere Bedingungen mit unterschiedlichen Sucheinstellungen erstellen. Beispielsweise können Sie zwei Bedingungen erstellen und in jeder davon unterschiedliche IP-Bereiche festlegen. Wenn mehrere Bedingungen festgelegt werden, zeigt eine Auswahl die Geräte an, die eine der Bedingungen erfüllen. Im Gegensatz dazu werden Sucheinstellungen innerhalb einer Bedingung übereinandergelegt. Wenn sowohl ein IP-Bereich als auch der Name einer installierten Anwendung in einer Bedingung festgelegt sind, werden nur jene Geräte angezeigt, bei denen sowohl die Anwendung installiert ist als auch die IP-Adresse zum festgelegten Bereich gehört.

Geräteliste einer Geräteauswahl anzeigen

In Kaspersky Security Center Linux können Sie die Liste der Geräte für eine Geräteauswahl anzeigen.

So zeigen Sie die Geräteliste für die Geräteauswahl an:

1. Gehen Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung** → **Geräteauswahlen** oder **Gerätesuche und Bereitstellung** → **Geräteauswahlen**.

2. Klicken Sie in der Auswahlliste auf den Namen der entsprechenden Geräteauswahl.

   Auf der Seite wird eine Tabelle mit Informationen über die Geräte angezeigt, die in der Geräteauswahl enthalten sind.

3. Sie können die Tabelle mit den Geräten wie folgt gruppieren und filtern:

   - Klicken Sie auf das Einstellungssymbol (⚙) und wählen Sie anschließend die Spalten aus, die in der Tabelle angezeigt werden sollen.

   - Klicken Sie auf das Filter-Symbol (▽), geben Sie im aufgerufenen Menü das Filterkriterium an und wenden Sie es an.

     Die gefilterte Tabelle der Geräte wird angezeigt.

Sie können in der Geräteauswahl mehrere Geräte auswählen und auf die Schaltfläche **Neue Aufgabe** klicken, um eine Aufgabe zu erstellen, die auf diese Geräte angewendet wird.

Um die ausgewählten Geräte der Geräteauswahl in eine andere Administrationsgruppe zu verschieben, klicken Sie auf die Schaltfläche **In Gruppe verschieben** und wählen Sie anschließend die Ziel-Administrationsgruppe aus.

Geräteauswahl erstellen

Um eine Geräteauswahl zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Geräteauswahlen**.

   Eine Seite mit einer Liste von Geräteauswahlen wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Einstellungen der Geräteauswahl** wird geöffnet.

3. Geben Sie den Namen der neuen Auswahl ein.

4. Geben Sie die Gruppe mit den Geräten a, die in die Geräteauswahl aufgenommen werden sollen:

   - **Alle Geräte suchen** – Es wird nach Geräten gesucht, welche die Auswahlkriterien erfüllen und die entweder zur Gruppe **Verwaltete Geräte** oder zur Gruppe **Nicht zugeordnete Geräte** gehören.
   - **Verwaltete Geräte suchen** – Es wird nach Geräten gesucht, welche die Auswahlkriterien erfüllen und die zur Gruppe **Verwaltete Geräte** gehören.
   - **Nicht zugeordnete Geräte suchen** – Es wird nach Geräten gesucht, welche die Auswahlkriterien erfüllen und die zur Gruppe **Nicht zugeordnete Geräte** gehören.

   Sie können das Kontrollkästchen **Daten von sekundären Administrationsservern einbeziehen** aktivieren, um die Suche nach Geräten zu aktivieren, welche die Auswahlkriterien erfüllen und von sekundären Administrationsservern verwaltet werden.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**.

6. Wechseln Sie in das neue Fenster, geben Sie Bedingungen an, die erfüllt sein müssen, um Geräte in diese Auswahl aufzunehmen, und klicken Sie auf **OK**.

7. Klicken Sie auf die Schaltfläche **Speichern**.

Die Geräteauswahl wurde erstellt und der Liste mit Geräteauswahlen hinzugefügt.

Einstellungen einer Geräteauswahl anpassen

Um die Einstellungen für eine Geräteauswahl anzupassen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Geräteauswahlen**.

   Eine Seite mit einer Liste von Geräteauswahlen wird angezeigt.

2. Wählen Sie die relevante benutzerdefinierte Geräteauswahl aus und klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Fenster **Einstellungen der Geräteauswahl** wird geöffnet.

3. Klicken Sie auf der Registerkarte **Allgemein** auf den Link **Neue Bedingung**.

4. Geben Sie Bedingungen an, die erfüllt sein müssen, damit Geräte in die Auswahl aufgenommen werden.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die Einstellungen werden übernommen und gespeichert.

Nachfolgende werden die Einstellungen für Bedingungen der Aufnahme von Geräten in die Auswahl beschrieben. Die Bedingungen beruhen auf dem logischen ODER: In die Auswahl werden nur Geräte aufgenommen, die mindestens eine Bedingung erfüllen.

Allgemein

Im Abschnitt **Allgemein** kann der Name der Auswahlbedingung geändert sowie bestimmt werden, ob diese Auswahlbedingung umgekehrt werden soll:

Auswahlbedingung umkehren

Diese Option ist standardmäßig deaktiviert.

Wenn Sie diese Option aktivieren, wird die vorgegebene Auswahlbedingung umgekehrt. Alle Geräte, die diese Bedingung nicht erfüllen, werden in die Auswahl aufgenommen.

Das folgende Beispiel erläutert die Logik einer Inversion:

- **Bedingung**: Auf Ihrem Gerät befindet sich ein Betriebssystem, das zu den Linux-Systemen gehört und die Build-Nummer 00.0.000 besitzt.
- **Invertierter Zustand**: Auf Ihrem Gerät befindet sich ein Betriebssystem, dass NICHT (zu den Linux-Systemen gehört und die Build-Nummer 00.0.000 besitzt), was Folgendem entspricht:

  Es ist ein Betriebssystem vorhanden, das NICHT zu den Linux-Systemen gehört ODER das NICHT die Build-Nummer 00.0.000 besitzt.

Die Auswahl umfasst also beispielhaft Geräte mit Windows-Betriebssystemen mit der Build-Nummer 00.0.000 oder Geräte mit Linux-Betriebssystemen mit einer Build-Nummer, die von 00.0.000 abweicht.

Netzwerkinfrastruktur

Im Unterabschnitt **Netzwerk** können Sie die Bedingungen für die Aufnahme von Geräten anhand ihrer Netzwerkdaten konfigurieren:

- **Gerätename**

  Windows-Netzwerkname (NetBIOS-Name) des Geräts oder die IPv4- oder IPv6-Adresse.

- **Domäne**

  Es werden alle Geräte angezeigt, die zur angegebenen Arbeitsgruppe gehören.

- **Administrationsgruppe**

  Es werden Geräte angezeigt, die zur angegebenen Administrationsgruppe gehören.

- **Beschreibung**

  Text im Eigenschaftenfenster des Gerätes: im Feld **Beschreibung** von Abschnitt **Allgemein**.

  Für die Beschreibung eines Textes im Feld **Beschreibung** sind die folgenden Zeichen zulässig:

  - Innerhalb eines Wortes:

    - *****. Dieses Zeichen ersetzt beliebige Ausdrücke mit einer beliebigen Zahl von Zeichen.

    Beispiel:

    Für die Beschreibung der Wörter **Server** und **Server-**können Sie die Zeichenfolge **Server*** verwenden.

    - **?.** Dieses Zeichen ersetzt ein beliebiges Symbol.

Beispiel:

Um Phrasen wie **SUSE Linux Enterprise-Server 12** oder **SUSE Linux Enterprise-Server 15** zu beschreiben, können Sie **SUSE Linux Enterprise-Server 1?** eingeben.

Das Zeichen ***** oder **?** kann nicht als das erste Zeichen in einer Textbeschreibung verwendet werden.

- Zur Verknüpfung mehrerer Wörter:

  - Leerzeichen: Es werden alle Geräte angezeigt, deren Beschreibung ein beliebiges der angegebenen Wörter enthält.

  Beispiel:

  Zur Beschreibung einer Phrase, die entweder das Wort **Sekundär** oder **Virtuell** enthält, können Sie die Zeichenfolge **Sekundär Virtuell** verwenden.

  - **+**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort unbedingt im Text vorhanden sein muss.

  Beispiel:

  Zur Beschreibung einer Phrase, welche die beiden Wörter **Sekundär** und **Virtuell** enthält, können Sie den Ausdruck **+Sekundär+Virtuell** verwenden.

  - **-**: Vor einem Wort stehend bedeutet dieses Zeichen, dass das Wort im Suchtext nicht vorkommen darf.

  Beispiel:

  Zur Beschreibung einer Phrase, die das Wort **Sekundär** enthält, jedoch das Wort **Virtuell** nicht enthalten darf, können Sie den Ausdruck **+Sekundär-Virtuell** verwenden.

  - **"<Textabschnitt>"**: Ein in Anführungszeichen eingeschlossener Textabschnitt muss vollständig im Text vorhanden sein.

  Beispiel:

  Zur Beschreibung einer Phrase, welche die Wortverbindung **Sekundärer Server** enthält, können Sie den Ausdruck **"Sekundärer Server"** verwenden.

- **IP-Bereich**

  Wenn diese Option aktiviert ist, können Sie in den Eingabefeldern die erste und die letzte IP-Adresse des Bereichs eingeben, zu dem die betreffenden Geräte gehören sollen.

  Diese Option ist standardmäßig deaktiviert.

- **Verwaltung erfolgt durch anderen Administrationsserver**

  Wählen Sie eine der folgenden Werte aus:

  - **Ja**. Eine Verschiebungsregel gilt nur für Client-Geräte, die von anderen Administrationsservern verwaltet werden. Diese Server unterscheiden sich von dem Server, auf dem Sie die Verschiebungsregel für Geräte konfigurieren.

  - **Nein**. Die Verschiebungsregel gilt nur für Client-Geräte, die vom aktuellen Administrationsserver verwaltet werden.

  - **Es wurde kein Wert gewählt**. Die Bedingung trifft nicht zu.

Im Unterabschnitt **Domänencontroller** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand ihrer Domänenmitgliedschaft anpassen:

- **Gerät befindet sich in einer Domänen-Organisationseinheit**

  Wenn diese Option aktiviert ist, werden in die Auswahl Geräte aus der Domänenorganisationseinheit aufgenommen, die im Eingabefeld angegeben wurde.

  Diese Option ist standardmäßig deaktiviert.

- **Gerät ist Mitglied der Domänen-Sicherheitsgruppe**

  Wenn diese Option aktiviert ist, werden in die Auswahl Geräte aus der Domänensicherheitsgruppe aufgenommen, die im Eingabefeld angegeben wurde.

  Diese Option ist standardmäßig deaktiviert.

Im Unterabschnitt **Netzwerkaktivität** können Sie die Bedingungen für die Aufnahme von Geräten anhand ihrer Netzwerkaktivitäten konfigurieren:

- **Fungiert als Verteilungspunkt**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Bei Auswahl dieser Option werden Geräte, die als Verteilungspunkte fungieren, in die Auswahl aufgenommen.
  - **Nein**. Geräte, die als Verteilungspunkte fungieren, werden nicht in die Auswahl aufgenommen.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Verbindung mit Administrationsserver nicht trennen**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Aktiviert**. Zur Auswahl gehören die Geräte, auf denen das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** aktiviert ist.
  - **Deaktiviert**. Zur Auswahl gehören die Geräte, auf denen das Kontrollkästchen **Verbindung mit Administrationsserver nicht trennen** deaktiviert ist.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Das Verbindungsprofil wurde gewechselt**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Bei Auswahl dieser Option werden Geräte, die infolge eines Wechsels des Verbindungsprofils mit dem Administrationsserver verbunden wurden, in die Auswahl aufgenommen.
  - **Nein**. Geräte, die infolge eines Wechsels des Verbindungsprofils mit dem Administrationsserver verbunden wurden, werden nicht in die Auswahl aufgenommen.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Letzte Verbindung mit dem Administrationsserver**

  Mithilfe dieses Kontrollkästchens können Sie ein Kriterium für die Suche von Geräten anhand des Zeitpunkts der letzten Verbindung mit dem Administrationsserver ausführen.

  Wenn dieses Kontrollkästchen aktiviert ist, können Sie in den Eingabefeldern die Werte des Zeitraums (Datum und Uhrzeit) angeben, während dessen die letzte Verbindung des auf dem Client-Gerät installierten Administrationsagenten mit dem Administrationsserver hergestellt wurde. Bei Auswahl dieser Option werden in die Auswahl Geräte aufgenommen, die dem festgelegten Zeitraum entsprechen.

  Ist das Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Neue Geräte bei der Netzwerkabfrage erkannt**

  Suche nach neuen Geräten, die während der letzten Tage bei der Netzwerkabfrage gefunden wurden.

  Wenn diese Option aktiviert ist, umfasst die Auswahl nur neue Geräte, die bei einer Gerätesuche während der im Feld **Erkennungszeitraum (Tage)** angegebenen Anzahl von Tagen gefunden wurden.

  Ist die Option deaktiviert, umfasst die Auswahl alle Geräte, die bei einer Gerätesuche gefunden wurden.

  Diese Option ist standardmäßig deaktiviert.

- **Gerät ist sichtbar**

  In dieser Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl bei der Suche wählen:

  - **Ja**. Es werden Geräte in die Auswahl aufgenommen, die momentan im Netzwerk sichtbar sind.
  - **Nein**. Die Anwendung nimmt Geräte in die Auswahl auf, die momentan nicht im Netzwerk sichtbar sind.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

Gerätestatus

Im Unterabschnitt **Status des verwalteten Geräts** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Beschreibung des Gerätestatus der verwalteten Anwendung anpassen:

- **Gerätestatus**

  In dieser Dropdown-Liste können Sie einen Gerätestatus auswählen: *OK*, *Kritisch* oder *Warnung*.

- **Status des Echtzeitschutzes**

  In dieser Dropdown-Liste können Sie den Wert für den Status des Echtzeitschutzes auswählen. Geräte mit dem angegebenen Echtzeitschutz-Status werden in die Auswahl aufgenommen.

- **Beschreibung des Gerätestatus**

  In diesem Feld können Sie die Kontrollkästchen für jene Bedingungen aktivieren, auf deren Basis einem Gerät eine der folgenden Statusvarianten zugewiesen werden soll: *OK, Kritisch* oder *Warnung*.

Im Unterabschnitt **Status der Komponenten der verwalteten Anwendungen** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Statuswerte der Komponenten der verwalteten Anwendungen anpassen:

- **Status des Schutzes vor Datenverlust**

  Suche nach Geräten anhand des Status des "Schutzes vor Datenverlust" (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- **Schutzstatus der Server für die Zusammenarbeit**

  Suche nach Geräten anhand des Status der Komponente "Schutz der Serverzusammenarbeit" (*Unbekannt*, *Beendet*, *Wird gestartet, Angehalten*, *Wird ausgeführt*, *Fehlgeschlagen*).

- **Antiviren-Schutzstatus der Mail-Server**

  Suche nach Geräten anhand des Status des Mail-Server-Schutzes (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

- **Status der Komponente "Endpoint Sensor"**

  Suche nach Geräten anhand des Status der Komponente "Endpoint Sensor" (*Unbekannt, Beendet, Wird gestartet, Angehalten, Wird ausgeführt, Fehlgeschlagen*).

Im Unterabschnitt **Statusbeeinflussende Probleme in verwalteten Anwendungen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Liste von möglichen von einer verwalteten Anwendung gefundenen Problemen anpassen. Wenn zumindest ein ausgewähltes Problem auf einem Gerät existiert, wird das Gerät in die Auswahl aufgenommen. Wenn Sie ein Problem auswählen, das für mehrere Anwendungen aufgelistet ist, haben Sie die Möglichkeit, dieses Problem in allen Listen automatisch auszuwählen.

Sie können die Kontrollkästchen für die Beschreibung der Status der verwalteten Anwendungen aktivieren, bei deren Empfang die Geräte in die Auswahl aufgenommen werden. Wenn Sie einen Status auswählen, der für mehrere Anwendungen aufgelistet ist, haben Sie die Möglichkeit, diesen Status in allen Listen automatisch auszuwählen.

Details zum System

Im Abschnitt **Betriebssystem** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl auf der Grundlage des darauf installierten Betriebssystems anpassen.

- **Plattformtyp**

  Ist das Kontrollkästchen aktiviert, können Sie Betriebssysteme in der Liste auswählen. Geräte, auf denen die angegebenen Betriebssysteme installiert sind, werden in die Suchergebnisse aufgenommen.

- **Service Pack-Version des Betriebssystems**

  In diesem Feld können Sie die Service Pack-Version (im Format *X.Y*) des Betriebssystems angeben, die bestimmt, wie die Verschiebungsregel auf das Gerät angewendet wird. Standardmäßig ist keine Version angegeben.

- **Architektur des Betriebssystems**

  In dieser Dropdown-Liste können Sie die Architektur des Betriebssystems auswählen, die vorhanden sein muss, damit auf dem Gerät die Regel für das Verschieben angewandt wird (**Unbekannt**, **x86**, **AMD64**, **IA64**). Standardmäßig ist in dieser Liste keine Variante ausgewählt, die Architektur des Betriebssystems ist nicht angegeben.

- **Build des Betriebssystems**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Versionsnummer des Betriebssystems. Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Versionsnummer haben muss. Sie können auch eine Suche nach allen Versionsnummern mit Ausnahme der angegebenen anpassen.

- **Release-Nummer des Betriebssystems**

  > Diese Einstellung ist nur auf Windows-Betriebssysteme anwendbar.

  Release-Identifikator (ID) des Betriebssystems Sie können festlegen, ob das ausgewählte Betriebssystem eine gleiche, frühere oder spätere Release-ID haben muss. Sie können auch eine Suche nach allen Release-ID-Nummern mit Ausnahme der angegebenen anpassen.

Auf der Registerkarte **Virtuelle Maschinen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anpassen, je nachdem, ob diese Geräte virtuelle Maschinen sind oder zur Virtual Desktop Infrastructure (VDI) gehören:

- **Ist eine virtuelle Maschine**

  Sie können in der Dropdown-Liste folgende Elemente wählen:

  - **Nicht definiert**.
  - **Nein**. Die gesuchten Geräte dürfen keine virtuellen Maschinen sein.
  - **Ja**. Die gesuchten Geräte müssen virtuelle Maschinen sein.

- **Typ der virtuellen Maschine**

  In der Dropdown-Liste können Sie den Hersteller der virtuellen Maschine auswählen.

  Die Dropdown-Liste ist verfügbar, wenn die Werte **Ja** oder **Unwichtig** in der Dropdown-Liste **Dies ist eine virtuelle Maschine** gewählt wurden.

- **Teil einer Virtual Desktop Infrastructure (VDI)**

  Sie können in der Dropdown-Liste folgende Elemente wählen:

  - **Nicht definiert**.
  - **Nein**. Die gesuchten Geräte dürfen kein Teil der Virtual Desktop Infrastructure (VDI) sein.
  - **Ja**. Die gesuchten Geräte müssen Teil der Virtual Desktop Infrastructure (VDI) sein.

Im Unterabschnitt **Hardware-Register** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der auf ihnen installierten Hardware anpassen:

Stellen Sie sicher, dass das Tool "lshw" auf den Linux-Geräten installiert ist, von denen Sie die Hardwaredetails abrufen möchten. Die von virtuellen Maschinen abgerufenen Hardwaredetails können je nach verwendetem Hypervisor unvollständig sein.

- **Gerät**

  In dieser Dropdown-Liste können Sie einen Einheitentyp auswählen. Alle Geräte mit dieser Einheit werden in die Suchergebnisse aufgenommen.

  Im Feld wird die Volltextsuche unterstützt.

- **Hersteller**

  In dieser Dropdown-Liste können Sie den Namen eines Herstellers der Einheit auswählen. Alle Geräte mit dieser Einheit werden in die Suchergebnisse aufgenommen.

  Im Feld wird die Volltextsuche unterstützt.

- **Gerätename**

  Ein Gerät mit dem angegebenen Namen wird in die Auswahl aufgenommen.

- **Beschreibung**

  Beschreibung des Geräts oder der Hardware. Geräte mit der in diesem Feld angegebenen Beschreibung werden in die Auswahl aufgenommen.

  Eine Beschreibung in beliebiger Form kann im Fenster Geräteeigenschaften eingegeben werden. Im Feld wird die Volltextsuche unterstützt.

- **Gerätehersteller**

  Bezeichnung des Geräteherstellers. Geräte, die vom angegebenen Hersteller produziert wurden, werden in die Auswahl aufgenommen.

  Der Name des Herstellers kann im Fenster Geräteeigenschaften eingegeben werden.

- **Seriennummer**

  Hardware mit in diesem Feld angegebener Seriennummer wird in die Auswahl aufgenommen.

- **Inventarnummer**

  Hardware mit in diesem Feld angegebener Inventarnummer wird in die Auswahl aufgenommen.

- **Benutzer**

  Hardware des in diesem Feld angegebenen Benutzers wird in die Auswahl aufgenommen.

- **Ort**

  Standort des Geräts bzw. der Hardware (z. B. im Büro oder in der Filiale). Computer oder andere Geräte am in diesem Feld angegebenen Ort werden in die Auswahl aufgenommen.

  Der Ort der Hardware kann in beliebiger Form im Hardware-Eigenschaftenfenster eingegeben werden.

- **CPU-Taktrate in MHz, von**

  Die minimale Taktrate einer CPU. Geräte mit einer CPU, deren Taktrate dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **CPU-Taktrate MHz, bis**

  Die maximale Taktrate einer CPU. Geräte mit einer CPU, deren Taktrate dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Anzahl virtueller CPU-Kerne, von**

  Die minimale Anzahl an virtuellen CPU-Kernen. Geräte mit einer CPU, deren Anzahl an Kernen dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Anzahl virtueller CPU-Kerne, bis**

  Die maximale Anzahl an virtuellen CPU-Kernen. Geräte mit einer CPU, deren Anzahl an Kernen dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Größe der Festplatte (GB), von**

  Die minimale Größe der Festplatte des Geräts. Geräte mit Festplatten, deren Größe dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Größe der Festplatte (GB), bis**

  Die maximale Größe der Festplatte des Geräts. Geräte mit Festplatten, deren Größe dem Bereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Größe des Arbeitsspeichers (MB), von**

  Die minimale Größe des Arbeitsspeichers des Geräts. Geräte mit Arbeitsspeicher, der dem Größenbereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

- **Größe des Arbeitsspeichers (MB), bis**

  Die minimale Größe des Arbeitsspeichers des Geräts. Geräte mit Arbeitsspeicher, der dem Größenbereich in den Eingabefeldern entspricht (inklusive), werden in die Auswahl aufgenommen.

Details zu Drittherstellersoftware

Im Unterabschnitt **Programm-Registry** können Sie die Kriterien für die Aufnahme von Geräten anhand von installierten Anwendungen anpassen:

- **Anwendungsname**

  In dieser Dropdown-Liste können Sie einen Anwendungsnamen auswählen. Die Geräte, auf denen diese Anwendung installiert ist, werden in die Auswahl aufgenommen.

- **Anwendungsversion**

  Geben Sie in diesem Eingabefeld die Version der ausgewählten Anwendung ein.

- **Hersteller**

  In dieser Dropdown-Liste können Sie den Hersteller der auf dem Gerät installierten Anwendung auswählen.

- **Anwendungsstatus**

  Dropdown-Liste, in der Sie den Status der Anwendung auswählen können (*Installiert*, *Nicht installiert*). Die Geräte, auf denen die angegebene Anwendung abhängig vom ausgewählten Status installiert bzw. nicht installiert ist, werden in die Auswahl aufgenommen.

- **Nach Update suchen**

  Wenn diese Option aktiviert ist, erfolgt die Suche anhand der Updatedaten der auf den Geräten installierten Anwendungen. Nachdem Sie das Kontrollkästchen aktiviert haben, ändern sich die Felder **Anwendungsname**, **Anwendungsversion** und **Anwendungsstatus** in **Update-Name**, **Update-Version** und **Status**.

  Diese Option ist standardmäßig deaktiviert.

- **Name der inkompatiblen Sicherheitsanwendung**

  In dieser Dropdown-Liste können Sie Sicherheitsanwendungen von Drittanbietern auswählen. Bei der Suche werden Geräte in die Auswahl aufgenommen, auf denen die ausgewählte Anwendung installiert wurde.

- **Anwendungs-Tag**

  In dieser Dropdown-Liste können Sie ein Anwendungs-Tag auswählen. Alle Geräte, auf denen Anwendungen installiert sind, die das ausgewählte Tag in der Beschreibung haben, werden in die Geräteauswahl aufgenommen.

- **Gilt für Geräte ohne die angegebenen Tags**

  Wenn diese Option aktiviert ist, werden Geräte, in deren Beschreibung keines der gewählten Tags vorkommt, in die Auswahl aufgenommen.

  Wenn diese Option deaktiviert ist, wird das Kriterium nicht angewendet.

  Diese Option ist standardmäßig deaktiviert.

Im Unterabschnitt **Schwachstellen und Updates** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Quelle der Windows-Updates anpassen:

WUA wurde auf den Administrationsserver umgeschaltet

In dieser Dropdown-Liste können Sie eine der folgenden Varianten der Suche auswählen:

- **Ja**. Bei Auswahl dieser Option werden Geräte in die Suchergebnisse aufgenommen, die Windows-Updates vom Administrationsserver herunterladen.
- **Nein**. Bei Auswahl dieser Option werden Geräte in die Ergebnisse aufgenommen, die Windows-Updates von einer anderen Quelle herunterladen.

Details zu Kaspersky-Anwendungen

Im Unterabschnitt **Kaspersky-Anwendungen** können Sie die Kriterien für die Aufnahme von Geräten anhand der ausgewählten verwalteten Anwendung konfigurieren:

- **Anwendungsname**

  In der Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl wählen, wenn die Suche anhand des Namens der Kaspersky-Anwendung erfolgt.

  In der Liste sind nur die Anwendungen aufgeführt, für die Verwaltungs-Plug-ins im Administrator-Arbeitsplatz installiert sind.

  Wurde keine Anwendung gewählt, wird kein Kriterium angewandt.

- **Anwendungsversion**

  In diesem Eingabefeld können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl angeben, wenn die Suche nach Versionsnummer der Kaspersky-Anwendung erfolgt.

  Wurde keine Versionsnummer angegeben, wird kein Kriterium angewandt.

- **Name des kritischen Updates**

  In diesem Eingabefeld können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl angeben, wenn die Suche nach dem Namen der Anwendung oder nach der Update-Paketnummer erfolgt.

  Ist dieses Feld leer, wird kein Kriterium angewandt.

- **Programm-Status**

  Dropdown-Liste, in der Sie den Status der Anwendung auswählen können (*Installiert*, *Nicht installiert*). Die Geräte, auf denen die angegebene Anwendung abhängig vom ausgewählten Status installiert bzw. nicht installiert ist, werden in die Auswahl aufgenommen.

- **Wählen Sie den Zeitraum für das letzte Modul-Update**

  Mithilfe dieser Option können Sie ein Kriterium für die Suche nach Geräten nach Uhrzeit des letzten Updates der Programm-Module angeben, die auf den Geräten installiert wurden.

  Ist das Kontrollkästchen aktiviert, können Sie in den Eingabefeldern die Werte des Zeitraums (Datum und Uhrzeit) angeben, in dem das letzte Update der auf den Geräten installierten Anwendungsmodule ausgeführt wurde.

  Ist das Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Das Gerät wird durch den Administrationsserver verwaltet**

  Mithilfe dieser Dropdown-Liste können Geräte in die Auswahl aufgenommen werden, die über Kaspersky Security Center Linux verwaltet werden:

  - **Ja**. Geräte werden in die Auswahl aufgenommen, wenn sie über Kaspersky Security Center Linux verwaltet werden.
  - **Nein**. Die Anwendung nimmt Geräte in die Auswahl auf, wenn sie nicht über Kaspersky Security Center Linux verwaltet werden.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

- **Sicherheitsanwendung wurde installiert**

  Mithilfe dieser Dropdown-Liste können Geräte in die Auswahl aufgenommen werden, auf denen eine Sicherheitsanwendung installiert wurde:

  - **Ja**. Geräte werden in die Auswahl aufgenommen, wenn auf ihnen eine Sicherheitsanwendung installiert ist.
  - **Nein**. Die Anwendung nimmt alle Geräte in die Auswahl auf, die keine Sicherheitsanwendung installiert haben.
  - **Es wurde kein Wert gewählt**. Es wird kein Kriterium angewandt.

Im Unterabschnitt **Antiviren-Schutz** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand des Schutzstatus anpassen:

- **Veröffentlichung der Datenbanken**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach dem Veröffentlichungsdatum der Antiviren-Datenbanken. In den Eingabefeldern können Sie den Zeitraum festlegen, anhand dessen die Suche ausgeführt werden soll.

  Diese Option ist standardmäßig deaktiviert.

- **Anzahl der Datenbank-Einträge**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach der Anzahl der Datenbank-Einträge. In den Eingabefeldern können Sie den unteren und oberen Wert für die Anzahl der Einträge in der Antiviren-Datenbank festlegen.

  Diese Option ist standardmäßig deaktiviert.

- **Letzte Virensuche**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach dem Zeitpunkt der letzten Schadsoftware-Untersuchung. In den Eingabefeldern können Sie den Zeitraum festlegen, in dem die Schadsoftware-Untersuchung zum letzten Mal erfolgte.

  Diese Option ist standardmäßig deaktiviert.

- **Gefundene Bedrohungen**

  Wenn diese Option aktiviert ist, erfolgt die Suche der Client-Geräte nach der Anzahl der gefundenen Viren. In den Eingabefeldern können Sie den unteren und oberen Wert für die Anzahl der gefundenen Viren festlegen.

  Diese Option ist standardmäßig deaktiviert.

Im Unterabschnitt **Verschlüsselung** können Sie das Kriterium für die Aufnahme von Geräten anhand des ausgewählten Verschlüsselungsalgorithmus konfigurieren:

Verschlüsselungsalgorithmus

Standard des symmetrischen Algorithmus der Blockverschlüsselung Advanced Encryption Standard (AES). In der Dropdown-Liste können Sie die Länge des Chiffrierschlüssels (56 Bit, 128 Bit, 192 Bit oder 256 Bit) auswählen.

AES56, *AES128*, *AES192*, *AES256*.

Der Unterabschnitt **Programmkomponenten** enthält eine Liste mit Komponenten von Anwendungen, für die entsprechende Verwaltungs-Plug-ins in Kaspersky Security Center Web Console installiert sind.

Im Unterabschnitt **Programmkomponenten** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Status und Versionsnummern der Komponenten festlegen, die sich auf die ausgewählte Anwendung beziehen:

- **Status**

  Suche nach Geräten anhand des Status der Komponente, der von einer Anwendung an den Administrationsserver gesendet wurde. Sie können einen der folgenden Statuswerte auswählen: *Keine Daten, Beendet*, *Angehalten*, *Wird gestartet*, *Wird ausgeführt, Fehlgeschlagen*, *Nicht installiert, Von der Lizenz nicht unterstützt*. Wenn die ausgewählte Komponente der auf einem verwalteten Gerät installierten Anwendung den angegebenen Status aufweist, wird das Gerät bei der Geräteauswahl berücksichtigt.

Von Anwendungen gesendete Status:

- *Beendet* – Die Komponente ist deaktiviert und funktioniert momentan nicht.
- *Angehalten* – Die Komponente wird angehalten, z. B. nachdem der Benutzer den Schutz in der verwalteten Anwendung angehalten hat.
- *Wird gestartet* – Die Komponente wird gerade initialisiert.
- *Wird ausgeführt* – Die Komponente ist aktiviert und funktioniert ordnungsgemäß.
- *Fehlgeschlagen* – Während des Betriebs der Komponente ist ein Fehler aufgetreten.
- *Nicht installiert*–Der Benutzer hat die Komponente während der Konfiguration der benutzerdefinierten Installation der Anwendung nicht für die Installation ausgewählt.
- *Von der Lizenz nicht unterstützt* – Die Lizenz gilt nicht für die ausgewählte Komponente.

Im Gegensatz zu anderen Statuswerten wird der Statuswert *Keine Daten* nicht von Anwendungen versendet. Diese Option zeigt, dass die Anwendungen über keine Informationen über den ausgewählten Status der Komponente aufweisen. Dies kann beispielsweise der Fall sein, wenn die ausgewählte Komponente zu keiner der auf dem Gerät installierten Anwendungen gehört oder wenn das Gerät ausgeschaltet ist.

- **Version**

  Suche nach Geräten anhand der Versionsnummer der in der Liste ausgewählten Komponente. Sie können eine Versionsnummer eingeben, beispielsweise `3.4.1.0`, und dann festlegen, ob die ausgewählte Komponente eine gleich, frühere oder spätere Version aufweisen muss. Sie können auch eine Suche nach allen Versionen mit Ausnahme der angegebenen anpassen.

Tags

Im Abschnitt **Tags** können Sie Bedingungen für die Aufnahme von Geräten in die Auswahl nach Schlüsselworten (Tags) anpassen, die zuvor zu den Beschreibungen der verwalteten Geräte hinzugefügt wurden:

Anwenden, wenn mindestens eins der ausgewählten Tags zutrifft

Ist die Option aktiviert, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibungen zumindest einer der gewählten Tags vorhanden ist.

Ist die Option deaktiviert, werden in den Suchergebnissen nur Geräte angezeigt, in deren Beschreibungen alle gewählten Tags vorhanden sind.

Diese Option ist standardmäßig deaktiviert.

Um dem Kriterium Tags hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie die Tags aus, indem Sie auf das Eingabefeld **Tag** klicken. Geben Sie an, ob die Geräte mit den ausgewählten Tags in die Geräteauswahl aufgenommen oder davon ausgeschlossen werden sollen.

- **Alle Geräte mit diesem Tag**

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

  Diese Variante ist standardmäßig ausgewählt.

- **Alle Geräte ohne dieses Tag**

  Wenn diese Variante ausgewählt ist, werden in den Suchergebnissen Geräte angezeigt, in deren Beschreibung der ausgewählte Tag nicht vorhanden ist. Bei der Gerätesuche können Sie das Zeichen * verwenden, um eine beliebige Zeile mit einer beliebigen Anzahl von Zeichen zu ersetzen.

Benutzer

Auf der Registerkarte **Benutzer** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Benutzerkonten anpassen, die sich am Betriebssystem angemeldet haben.

- **Letzter am System angemeldeter Benutzer**

  Wenn diese Option aktiviert ist, können Sie das Benutzerkonto für die Konfiguration des Kriteriums auswählen. In die Suchergebnisse werden Geräte aufgenommen, auf denen sich der ausgewählte Benutzer zuletzt angemeldet hat.

- **Benutzer, der sich mindestens einmal am System angemeldet hat**

  Ist diese Option aktiviert, können Sie durch Klicken auf die Schaltfläche **Durchsuchen** ein Benutzerkonto auswählen. In die Suchergebnisse werden Geräte aufgenommen, auf denen sich der angegebene Benutzer mindestens einmal im System angemeldet hat.

Gerätebesitzer

Im Abschnitt **Gerätebesitzer** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl nach registrierten Gerätebesitzern, deren Rollen und Sicherheitsgruppenmitgliedschaft festlegen:

- **Gerätebesitzer**

  Wählen Sie den Benutzernamen des Gerätebesitzers aus einer internen Sicherheitsgruppe aus. Weitere Informationen über Benutzer und Benutzerrollen finden Sie in diesem Abschnitt.

  > Es kann nur ein Benutzer als Gerätebesitzer registriert sein.

- **Zugehörigkeit des Gerätebesitzers zu einer Active Directory-Sicherheitsgruppe**

  Wählen Sie eine externe Active Directory-Sicherheitsgruppe aus, welcher der Gerätebesitzer angehört.

  > Der Benutzer kann entweder Teil einer Active Directory-Sicherheitsgruppe oder Teil einer Gruppe sein, die selbst zu der ausgewählten Active Directory-Sicherheitsgruppe gehört.

- **Rolle des Gerätebesitzers**

  Wählen Sie die Rolle aus, die dem Gerätebesitzer zugewiesen ist. Weitere Informationen über Benutzerrollen finden Sie in diesem Artikel.

- **Zugehörigkeit des Gerätebesitzers zu einer internen Sicherheitsgruppe**

  Wählen Sie eine interne Sicherheitsgruppe aus, welcher der Gerätebesitzer angehört.

Geräteliste einer Geräteauswahl exportieren

Mit der Kaspersky Security Center Linux können Sie Informationen über Geräte aus einer Geräteauswahl speichern und in eine csv- oder txt-Datei exportieren.

So exportieren Sie die Geräteliste der Geräteauswahl:

1. Öffnen Sie die Tabelle mit den Geräten aus der Geräteauswahl.
2. Verwenden Sie eine der folgenden Methoden, um die Geräte auszuwählen, die Sie exportieren möchten:
   - Um nur bestimmte Geräte auszuwählen, aktivieren Sie die entsprechenden Kontrollkästchen neben diesen.
   - Um alle Geräte auf der aktuellen Tabellenseite auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Gerätetabelle und aktivieren Sie anschließend das Kontrollkästchen **Alle auf aktueller Seite** auswählen.
   - Um alle Geräte aus der gesamten Tabelle auszuwählen, aktivieren Sie das Kontrollkästchen in der Kopfzeile der Gerätetabelle und aktivieren Sie dann das Kontrollkästchen **Alle auswählen**.
3. Klicken Sie auf die Schaltfläche **In csv-Datei exportieren** oder **In txt-Datei exportieren**. Alle Informationen zu den in der Tabelle enthaltenen ausgewählten Geräten werden exportiert.

Beachten Sie, dass bei einem auf die Tabelle angewendeten Filterkriterium nur die gefilterten Daten aus den angezeigten Spalten exportiert werden.

Geräte in der Auswahl aus Administrationsgruppen löschen

Bei der Arbeit mit einer Geräteauswahl können Sie Geräte direkt in der Auswahl aus den Administrationsgruppen löschen, ohne auf die Administrationsgruppen zu wechseln, aus denen die Geräte gelöscht werden sollen.

Um Geräte aus Administrationsgruppen zu löschen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Geräteauswahlen** oder zu **Gerätesuche und Bereitstellung** → **Geräteauswahlen**.
2. Klicken Sie in der Auswahlliste auf den Namen der entsprechenden Geräteauswahl.

   Auf der Seite wird eine Tabelle mit Informationen über die Geräte angezeigt, die in der Geräteauswahl enthalten sind.
3. Wählen Sie die Geräte aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.

   Daraufhin werden die gewählten Geräte aus den Administrationsgruppen gelöscht, zu denen sie gehörten.

Geräte-Tags

Kaspersky Security Center Linux erlaubt, den Geräten *Tags* zuzuweisen. Ein Tag ist eine Zeichenkette, die für die Gruppierung, Beschreibung oder Suche der Geräte verwendet werden kann. Die den Geräten zugewiesenen Tags können beim Erstellen von Geräteauswahlen, bei der Suche nach Geräten und bei der Gerätezuordnung anhand von Administrationsgruppen verwendet werden.

Die Tags können den Geräten manuell oder automatisch zugewiesen werden. Wenn Sie ein einzelnes Gerät mit Tags versehen möchten, können Sie die manuelle Tag-Zuweisung verwenden. Die automatische Tag-Zuweisung wird von Kaspersky Security Center Linux auf eine der folgenden Arten durchgeführt:

- In Übereinstimmung mit den angegebenen Regeln zur Tag-Zuweisung.
- Durch eine Anwendung.

Es wird nicht empfohlen, verschiedene Arten der Tag-Zuweisung zu verwenden, um dasselbe Tag zuzuweisen. Wenn das Tag beispielsweise durch die Regel zugewiesen wird, wird es nicht empfohlen, dieses Tag den Geräten manuell zuzuweisen.

Wenn die Tags durch Regeln zugewiesen werden, bekommen die Geräte die Tags zugewiesen, wenn die festgelegten Regeln erfüllt sind. Jedem Tag entspricht eine separate Regel. Die Regeln können auf die Netzwerkeigenschaften des Geräts, das Betriebssystem, die auf dem Gerät installierten Anwendungen und andere Eigenschaften des Geräts angewendet werden. Beispielsweise können Sie eine Regel konfigurieren, nach der allen Geräten, die unter dem Betriebssystem CentOS laufen, das Tag `[CentOS]` zugewiesen wird. Dieses Tag kann anschließend beim Erstellen einer Geräteauswahl verwendet werden, die Sie dabei unterstützt, alle CentOS-Geräte auszuwählen und diesen eine Aufgabe zuzuweisen.

Sie können pro Tag nur eine Regel für die automatische Tag-Zuweisung hinzufügen. Wenn Sie eine neue Regel für dasselbe Tag erstellen, wird die vorherige ersetzt.

Ein Tag wird in den folgenden Fällen automatisch vom Gerät entfernt:

- Wenn das Gerät nicht mehr die Bedingungen der Regel erfüllt, die das Tag zuweist.
- Wenn die Regel, die das Tag zuweist, deaktiviert oder gelöscht wird.

Die Liste der Tags und die Liste mit Regeln sind auf jedem Administrationsserver unabhängig von allen anderen Administrationsservern, einschließlich des primären Administrationsservers und der untergeordneten virtuellen Administrationsserver. Eine Regel wird nur auf Geräte des gleichen Administrationsservers angewendet, auf dem die Regel erstellt wurde.

Geräte-Tag erstellen

Um ein Geräte-Tag zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Tags** → **Tags des Geräts**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
   Ein neues Tag-Fenster öffnet sich.
3. Geben Sie im Feld **Tag** den Namen des Tags ein.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Das neue Tag wird in der Liste der Geräte-Tags angezeigt.

Geräte-Tag umbenennen

Um ein Geräte-Tag umzubenennen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Tags** → **Tags des Geräts**.
2. Klicken Sie auf den Namen des Tags, das Sie umbenennen möchten.
   Ein Fenster mit den Tag-Eigenschaften wird geöffnet.
3. Ändern Sie im Feld **Tag** den Tag-Namen.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Das aktualisierte Tag wird in der Liste der Geräte-Tags angezeigt.

Geräte-Tag löschen

Sie können nur manuell zugewiesene Tags löschen.

So löschen Sie ein manuell zugewiesenes Tag:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Tags** → **Tags des Geräts**.
   Die Liste der Tags wird angezeigt.
2. Wählen Sie das Geräte-Tag aus, den Sie löschen möchten.

3. Klicken Sie auf die Schaltfläche **Löschen**.

4. Klicken Sie im folgenden Fenster auf **Ja**.

   Das Geräte-Tag wird gelöscht. Das gelöschte Tag wird automatisch von allen Geräten entfernt, denen es zugewiesen war.

Wenn Sie ein Tag löschen, das dem Gerät durch eine Regel für die automatische Zuweisung von Tags zugewiesen wurde, wird die Regel nicht gelöscht und das Tag wird einem neuen Gerät zugewiesen, wenn das Gerät zum ersten Mal die Regelbedingungen erfüllt. Wenn Sie eine Regel für die automatische Tag-Kennzeichnung löschen, wird das in den Regelbedingungen angegebene Tag von allen Geräten, denen es zugewiesen wurde, entfernt. In der Tag-Liste bleibt es jedoch erhalten. Bei Bedarf können Sie das Tag manuell aus der Liste löschen.

Das gelöschte Tag wird nicht automatisch vom Gerät entfernt, wenn dieses Tag dem Gerät von einer Anwendung oder einem Administrationsagenten zugewiesen wurde. Verwenden Sie das Tool "klscflag", um solche Tags zu verwalten.

Geräte mit zugewiesenen Tags anzeigen

So zeigen Sie Geräte an, denen ein Tag zugewiesen ist:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Tags** → **Tags des Geräts**.

2. Klicken Sie auf den Link **Geräte anzeigen** neben dem Tag, für das Sie zugewiesene Geräte anzeigen möchten.

   Sie werden zum Abschnitt **Assets (Geräte)** des Hauptmenüs weitergeleitet, wobei die Geräte nach dem Tag gefiltert sind, auf dessen **Geräte anzeigen**-Link Sie geklickt haben.

3. Wenn Sie zur Liste der Geräte-Tags zurückzukehren möchten, klicken Sie in Ihrem Browser auf die Schaltfläche **Zurück**.

Nachdem Sie die Geräte mit dem zugewiesenen Tag angezeigt haben, können Sie entweder ein neues Tag erstellen und zuweisen oder das vorhandene Tag anderen Geräten zuweisen. In diesem Fall müssen Sie den Filterung nach Tag entfernen, die Geräte auswählen und anschließend das Tag zuweisen.

Tags anzeigen, die einem Gerät zugewiesen sind

So zeigen Sie einem Gerät zugewiesene Tags an:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.

2. Klicken Sie auf den Namen des Geräts, dessen Tags Sie anzeigen möchten.

3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Tags** aus.

   Die Liste der dem ausgewählten Gerät zugewiesenen Tags wird angezeigt. In der Spalte **Tag zugewiesen** können Sie anzeigen, wie das Tag zugewiesen wurde.

In der Werkzeugleiste sind folgende Aktionen möglich:

- Dem Gerät ein anderes Tag zuweisen.
- Ein bereits zugewiesenes Tag entfernen.
- Alle Geräte-Tags anzeigen, die auf dem Administrationsserver vorhanden sind.

Sie können die zugewiesenen Tags nicht lokal auf dem Gerät anzeigen.

Tags einem Gerät manuell zuweisen

So weisen Sie einem Gerät ein Tag manuell zu:

1. Zeigen Sie dem Gerät zugeordnete Tags an, dem Sie einen anderen Tag zuweisen möchten.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Führen Sie im folgenden Fenster einen der folgenden Schritte aus:
   - Um ein neues Tag zu erstellen und zuzuweisen, wählen Sie **Neues Tag erstellen** und geben Sie den Namen des neuen Tags ein.
   - Um ein vorhandenes Tag auszuwählen, wählen Sie **Vorhandenes Tag zuordnen** und dann in der Dropdown-Liste das gewünschte Tag.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu übernehmen.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Das ausgewählte Tag wird dem Gerät zugewiesen.

Zugewiesene Tags von einem Gerät entfernen

So entfernen Sie ein Tag von einem Gerät:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.
2. Klicken Sie auf den Namen des Geräts, dessen Tags Sie anzeigen möchten.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Tags** aus.
4. Aktivieren Sie das Kontrollkästchen neben dem Tag, das Sie entfernen möchten.

5. Klicken Sie am oberen Ende der Liste auf die Schaltfläche **Tag-Zuweisen aufheben**.
6. Klicken Sie im folgenden Fenster auf **Ja**.

   Das Tag wurde vom Gerät entfernt.

Das nicht zugewiesene Geräte-Tag wird nicht gelöscht. Bei Bedarf können Sie es manuell löschen.

Sie können Tags, die dem Gerät von Anwendungen oder Administrationsagenten zugewiesen wurden, nicht manuell entfernen. Um diese Tags zu verwalten, verwenden Sie das Tool "klscflag".

Regeln für das automatische Zuweisen von Tags an Geräten anzeigen

So zeigen Sie Regeln für die automatischer Zuweisung von Tags an Geräte an:

Führen Sie eine beliebige der folgenden Aktionen aus:

- Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Tags** → **Regeln für die automatische Tag-Zuweisung**.
- Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Tags** → **Tags des Geräts** und klicken Sie anschließend auf den Link **Regeln für die automatische Tag-Zuweisung einrichten**.
- Zeigen Sie die Tags an, die einem Gerät zugeordnet sind, und klicken Sie dann auf **Einstellungen**.

Die Liste der Regeln für die automatische Tag-Zuweisung von Geräten wird angezeigt.

Regeln für das automatische Zuweisen von Tags an Geräte bearbeiten

So bearbeiten Sie die Regeln für das automatische Zuweisen von Tags an Geräte:

1. Zeigen Sie die Regeln für das automatische Zuweisen von Tags an Geräte an.
2. Klicken Sie auf den Namen der Regel, die Sie bearbeiten möchten.

   Es wird ein Fenster zum Erstellen neuer Regeln geöffnet.
3. Bearbeiten Sie die allgemeinen Eigenschaften der Regel:

   a. Ändern Sie im Feld **Regelname** den Regelnamen.

   Der Name darf nicht mehr als 256 Zeichen enthalten.

b. Führen Sie eine beliebige der folgenden Aktionen aus:

- Aktivieren Sie die Regel, indem Sie die Umschaltfläche auf **Regel aktiviert** umschalten.
- Deaktivieren Sie die Regel, indem Sie die Umschaltfläche auf **Regel deaktiviert** umschalten.

4. Führen Sie eine beliebige der folgenden Aktionen aus:

- Um eine neue Bedingung hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**, um im sich öffnenden Fenster die Einstellungen der neuen Bedingung festzulegen.
- Um eine vorhandene Bedingung zu bearbeiten, klicken Sie auf den Namen dieser Bedingung und bearbeiten Sie dann die Einstellungen der Bedingung.
- Um eine Bedingung zu löschen, aktivieren Sie das Kontrollkästchen neben dem Namen dieser Bedingung und klicken Sie dann auf **Löschen**.

5. Klicken Sie im Fenster zum Einstellen der Bedingung auf **OK**.
6. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die bearbeitete Regel wird in der Liste angezeigt.

Regeln für das automatische Zuweisen von Tags an Geräte erstellen

So erstellen Sie Regeln für das automatische Zuweisen von Tags an Geräte:

1. Zeigen Sie die Regeln für das automatische Zuweisen von Tags an Geräte an.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Es wird ein neues Fenster zum Erstellen von Regeln geöffnet.
3. Passen Sie die allgemeinen Eigenschaften der Regel an:

   a. Geben Sie im Feld **Regelname** den Regelnamen ein.

   Der Name darf nicht mehr als 256 Zeichen umfassen.

   b. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie die Regel, indem Sie die Umschaltfläche auf **Regel aktiviert** umschalten.
   - Deaktivieren Sie die Regel, indem Sie die Umschaltfläche auf **Regel deaktiviert** umschalten.

   c. Geben Sie im Feld **Tag** den neuen Namen des Geräte-Tags ein oder wählen Sie eins der vorhandenen Geräte-Tags aus der Liste aus.

   Der Name darf nicht mehr als 256 Zeichen umfassen.
4. Klicken Sie im Abschnitt "Bedingungen" auf die Schaltfläche **Hinzufügen**, um eine neue Bedingung hinzufügen.

   Ein neues Fenster zum Einstellen von Bedingungen wird geöffnet.

5. Geben Sie den Namen der Bedingung ein.

   Der Name darf nicht mehr als 256 Zeichen umfassen. Der Name darf sich innerhalb einer Regel nicht wiederholen.

6. Passen Sie das Auslösen der Regel entsprechend den folgenden Bedingungen an: Es können mehrere Bedingungen ausgewählt werden.

   - **Netzwerk** – Netzwerkeigenschaften des Gerätes (beispielsweise DNS-Name des Gerätes oder Zugehörigkeit des Gerätes zu einem IP-Subnetz).

     Wenn für die Datenbank, die Sie für Kaspersky Security Center Linux verwenden, die Kollation zwischen Groß- und Kleinschreibung festgelegt ist, behalten Sie die Groß-/Kleinschreibung bei, wenn Sie einen DNS-Namen für das Gerät angeben. Andernfalls funktioniert Regel der automatischen Tag-Zuweisung nicht.

   - **Anwendungen** – Vorhandensein eines Administrationsagenten auf dem Gerät, Typ des Betriebssystems, Version, Architektur und Paketmanager.

   - **Virtuelle Maschinen** – Das Gerät gehört zu einem speziellen Typ für virtuelle Maschinen.

   - **Programm-Registry** – Vorhandensein von Anwendungen verschiedener Hersteller auf dem Gerät.

7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

   Falls erforderlich, können mehrere Bedingungen für eine Regel festgelegt werden. In diesem Fall wird den Geräten das Tag zugewiesen, wenn mindestens eine der Bedingungen erfüllt wird.

8. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die erstellte Regel wird auf Geräten ausgeführt, die vom ausgewählten Administrationsserver verwaltet werden. Wenn die Einstellungen für das Gerät den Bedingungen der Regel entsprechen, wird diesem Gerät das Tag zugewiesen.

Später wird eine Regel in folgenden Fällen angewendet:

- Automatisch und regelmäßig, abhängig von der Serverauslastung
- Nachdem Sie die Regel bearbeitet haben
- Wenn Sie die Regel manuell ausführen
- Wenn der Administrationsserver erkennt, dass entweder die Einstellungen eines Gerätes geändert wurden, das den Regelbedingungen entspricht, oder dass die Einstellungen einer Gruppe geändert wurden, zu der ein solches Gerät gehört.

Sie können mehrere Regeln zur Zuweisung von Tags erstellen. Einem Gerät können mehrere Tags zugewiesen werden, falls Sie mehrere Regeln zur Zuweisung von Tags erstellt haben und Bedingungen dieser Regeln gleichzeitig erfüllt sind. Sie können die Liste aller zugewiesenen Tags in den Eigenschaften des Geräts einsehen.

Regeln für das automatische Zuweisen von Tags an Geräte ausführen

Wird eine Regel ausgeführt, wird das in den Eigenschaften dieser Regel angegebene Tag den Geräten zugewiesen, welche die in den Eigenschaften derselben Regel angegeben Bedingungen erfüllen. Sie können nur aktivierte Regeln ausführen.

So führen Sie die Regeln für das automatische Zuweisen von Tags an Geräte aus:

1. Zeigen Sie die Regeln für das automatische Zuweisen von Tags an Geräte an.
2. Aktivieren Sie die Kontrollkästchen neben den aktivierten Regeln, die Sie ausführen möchten.
3. Klicken Sie auf die Schaltfläche **Regel ausführen**.

   Die ausgewählten Regeln werden ausgeführt.

Regeln für das automatische Zuweisen von Tags an Geräte löschen

So löschen Sie die Regeln für das automatische Zuweisen von Tags an Geräte:

1. Zeigen Sie die Regeln für das automatische Zuweisen von Tags an Geräte an.
2. Aktivieren Sie die Kontrollkästchen neben der Regel, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster erneut auf **Löschen**.

   Die ausgewählte Regel wird gelöscht. Das Tag, das in den Eigenschaften dieser Regel angegeben wurde, wird nicht von allen Geräten entfernt, denen es zugewiesen wurde.

> Das nicht zugewiesene Geräte-Tag wird nicht gelöscht. Bei Bedarf können Sie es manuell löschen.

Verwalten von Geräte-Tags mit dem Tool klscflag

Um einem Gerät einen Satz an Tags zuzuweisen, müssen Sie das Tool "klscflag" auf dem Client-Gerät ausführen, dem Sie die Tags zuweisen möchten.

Das Tool "klscflag" überschreibt die vorhandenen Tags, die dem Gerät zugewiesen sind. Dies bedeutet, dass Sie Tags hinzufügen oder entfernen können, indem Sie im Befehl den jeweiligen Satz an Tags angeben. Das Tool besitzt keine separaten Befehle zum Hinzufügen oder Entfernen einzelner Tags. Stattdessen ändern Sie den gesamten Satz an Tags.

Wenn Sie in Befehlen wie "klscflag" verschiedene Tag-Namen angeben, wird es empfohlen, einen einheitlichen Ansatz in Bezug auf die Groß- und Kleinschreibung zu wählen (z. B. ausschließlich Großbuchstaben für alle Tags). Je nach Konfiguration des DBMS hilft die ausschließliche Verwendung von Großbuchstaben bei der Vermeidung von Problemen mit Tags, die sich lediglich in der Groß- und Kleinschreibung unterscheiden.

So weisen Sie Ihrem Gerät Tags mithilfe des Tools "klscflag" zu:

1. Starten Sie die Eingabeaufforderung mit Root-Berechtigungen und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsagent installiert ist. Das Standardverzeichnis für die Installation ist /opt/kaspersky/klnagent64/sbin/.

2. Geben Sie einen der folgenden Befehle ein:

   - So weisen Sie einen Satz mit Tags zu:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" TAG-NAME_1 \",\" TAG-
     NAME_2 \",\" TAG-NAME_3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     wobei `[\" TAG-NAME_1 \",\" TAG-NAME_2 \",\" TAG-NAME_3 \"]` für die Liste der Tags steht, die Sie Ihrem Gerät zuweisen möchten.

     Wenn Sie die eckigen Klammern leer lassen, werden alle Tags vom Gerät entfernt:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type =
     \"SS_PRODINFO\";"
     ```

   - So weisen Sie einem vorhandenen Satz mit Tags ein neues Tag zu:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" NEUER-TAG-NAME \",\" TAG-
     NAME_1 \",\" TAG-NAME_2 \",\" TAG-NAME_3 \"]" -svt ARRAY_T -ss "|ss_type =
     \"SS_PRODINFO\";"
     ```

     wobei `NEUER-TAG-NAME` für den Namen des Tags steht, das Sie Ihrem Gerät zuweisen möchten, und `TAG-NAME_1`, `TAG-NAME_2` und `TAG-NAME_3` die Namen der Tags sind, die dem Gerät bereits zugewiesen sind.

   - Um ein bestimmtes Tag zu entfernen, ohne dabei andere, dem Gerät bereits zugewiesene, Tags zu entfernen, führen Sie den Befehl mit dem aktualisierten Satz an Tags aus.

     Wenn Ihre aktuellen Tags beispielsweise `TAG-NAME_1`, `TAG-NAME_2` und `TAG-NAME_3` lauten und Sie `TAG-NAME_2` entfernen möchten, führen Sie den folgenden Befehl aus:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" TAG-NAME_1 \",\" TAG-NAME_3 \"]" -
     svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. Starten Sie den Dienst des Administrationsagenten neu.

   Das Tool "klscflag" weist Ihrem Gerät die angegebenen Tags zu.

4. Wenn Sie sicherstellen möchten, dass die Tags durch das Tool "klscflag" erfolgreich zugewiesen wurden, zeigen Sie die dem Gerät zugewiesenen Tags an.

Alternativ können Sie Geräte-Tags manuell zuweisen.

Verschlüsselung und Datenschutz

Die Datenverschlüsselung verringert das Risiko eines unbeabsichtigten Verlusts sensibler Informationen und Unternehmensdaten, wenn Ihr Laptop oder Ihre Festplatte gestohlen wird oder verloren geht. Darüber hinaus können Sie mit der Datenverschlüsselung den Zugriff durch nicht autorisierte Benutzer und Anwendungen verhindern.

Sie können die Datenverschlüsselungsfunktion verwenden, wenn sich in Ihrem Netzwerk Windows-basierte verwaltete Geräte befinden, auf denen Kaspersky Endpoint Security für Windows installiert ist. In diesem Fall können Sie auf Geräten mit Windows-Betriebssystem die folgenden Arten von Verschlüsselungen verwalten:

- BitLocker-Laufwerkverschlüsselung
- Kaspersky-Festplattenverschlüsselung

Es wird nicht empfohlen, die Verschlüsselung in einer VDI-Umgebung zu aktivieren.

Durch die Verwendung dieser Komponenten von Kaspersky Endpoint Security für Windows können Sie beispielsweise die Verschlüsselung aktivieren oder deaktivieren, die Liste der verschlüsselten Laufwerke anzeigen oder Berichte über die Verschlüsselung erstellen und anzeigen.

Um die Verschlüsselung zu konfigurieren, definieren Sie in Kaspersky Security Center Linux die Richtlinien von Kaspersky Endpoint Security für Windows. Kaspersky Endpoint Security für Windows führt die Verschlüsselung und Entschlüsselung gemäß der aktiven Richtlinie aus. Ausführliche Anweisungen zur Konfiguration von Regeln und für eine Beschreibung der Verschlüsselungsfunktionen können Sie der Hilfe von Kaspersky Endpoint Security für Windows entnehmen.

Die Verschlüsselungsverwaltung ist für eine Hierarchie von Administrationsservern in der Web Console derzeit nicht verfügbar. Verwenden Sie den primären Administrationsserver, um verschlüsselte Geräte zu verwalten.

Mithilfe der Einstellungen der Benutzeroberfläche können Sie einige von den Elementen der Oberfläche, die sich auf die Funktion der Verschlüsselungsverwaltung beziehen, ein- und ausblenden.

Liste der verschlüsselten Laufwerke anzeigen

In Kaspersky Security Center Linux können Sie Details zu verschlüsselten Laufwerken und Geräten, die auf Laufwerksebene verschlüsselt sind, anzeigen. Wenn die Informationen auf einem Laufwerk entschlüsselt wurden, wird das Laufwerk automatisch aus der Liste entfernt.

Um die Liste der verschlüsselten Laufwerke anzuzeigen:

Gehen Sie im Hauptmenü zu **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselte Laufwerke**.

Wenn sich der Abschnitt nicht im Menü befindet, bedeutet dies, dass er ausgeblendet ist. Aktivieren Sie in den Einstellungen der Benutzeroberfläche die Option **Verschlüsselung und Datenschutz anzeigen**, um den Abschnitt anzuzeigen.

Sie können die Liste der verschlüsselten Laufwerke als csv- oder txt-Datei exportieren. Klicken Sie dazu entweder auf **In csv-Datei exportieren** oder auf **In txt-Datei exportieren**.

Liste der Verschlüsselungsereignisse anzeigen

Bei der Ausführung der Aufgaben zur Datenverschlüsselung oder -entschlüsselung auf den Client-Geräten sendet Kaspersky Endpoint Security für Windows an Kaspersky Security Center Linux Informationen über aufgetretene Ereignisse folgender Typen:

- Aufgrund unzureichenden Speicherplatzes kann eine Datei nicht verschlüsselt oder entschlüsselt werden oder ein verschlüsseltes Archiv nicht erstellt werden.
- Aufgrund eines Lizenzproblems kann eine Datei nicht verschlüsselt oder entschlüsselt werden oder ein verschlüsseltes Archiv nicht erstellt werden.
- Aufgrund fehlender Zugriffsrechte kann eine Datei nicht verschlüsselt oder entschlüsselt werden oder ein verschlüsseltes Archiv nicht erstellt werden.
- Das Zugreifen einer Anwendung auf eine verschlüsselte Datei wurde verweigert.
- Unbekannte Fehler.

Um sich eine Liste der Ereignisse anzeigen zu lassen, die bei einer Datenverschlüsselung auf Geräten aufgetreten sind, gehen Sie wie folgt vor:

Gehen Sie im Hauptmenü zu **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselungsereignisse**.

Wenn sich der Abschnitt nicht im Menü befindet, bedeutet dies, dass er ausgeblendet ist. Aktivieren Sie in den Einstellungen der Benutzeroberfläche die Option **Verschlüsselung und Datenschutz anzeigen**, um den Abschnitt anzuzeigen.

Sie können die Liste der verschlüsselten Laufwerke als csv- oder txt-Datei exportieren. Klicken Sie dazu entweder auf **In csv-Datei exportieren** oder auf **In txt-Datei exportieren**.

Alternativ können Sie die Liste der Verschlüsselungsereignisse für jedes verwaltete Gerät überprüfen.

So zeigen Sie die Verschlüsselungsereignisse eines verwalteten Geräts an:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.
2. Klicken Sie auf den Namen eines verwalteten Geräts.
3. Gehen Sie auf der Registerkarte **Allgemein** zum Abschnitt **Schutz**.
4. Klicken Sie auf den Link **Fehler der Datenverschlüsselung anzeigen**.

Verschlüsselungsberichte erstellen und anzeigen

Sie können folgende Berichte erstellen:

- Bericht über den Verschlüsselungsstatus verwalteter Geräte. Dieser Bericht enthält Details zur Datenverschlüsselung verschiedener verwalteter Geräte. Der Bericht zeigt beispielsweise die Anzahl der Geräte, für welche die Richtlinie mit konfigurierten Verschlüsselungsregeln gilt. Außerdem können Sie ihm entnehmen, wie viele Geräte neu gestartet werden müssen. Darüber hinaus enthält der Bericht Informationen über die Verschlüsselungstechnologie und den Algorithmus für jedes Gerät.

- Bericht über den Verschlüsselungsstatus der Massenspeichergeräte. Dieser Bericht enthält ähnliche Informationen wie der Bericht zum Verschlüsselungsstatus verwalteter Geräte, verfügt aber lediglich über Informationen zu Massenspeichergeräten und Wechseldatenträgern.

- Bericht über Zugriffsrechte auf verschlüsselte Laufwerke. Dieser Bericht zeigt, welche Benutzerkonten Zugriff auf verschlüsselte Laufwerke haben.

- Bericht über Fehler bei der Dateiverschlüsselung. Dieser Bericht enthält Informationen über Fehler, die bei der Ausführung der Aufgaben zur Verschlüsselung und Entschlüsselung von Daten auf den Client-Geräten aufgetreten sind.

- Bericht über blockierte Zugriffe auf verschlüsselte Dateien. Dieser Bericht enthält Informationen über das Blockieren des Zugriffs von Anwendungen auf verschlüsselte Dateien. Dieser Bericht ist hilfreich, wenn nicht autorisierte Benutzer oder Anwendungen versuchen, auf verschlüsselte Dateien oder Laufwerke zuzugreifen.

Im Abschnitt **Überwachung → Berichte** können Sie jeden Bericht generieren. Alternativ können Sie im Abschnitt **Vorgänge → Verschlüsselung und Datenschutz** die folgenden Verschlüsselungsberichte generieren:

- Bericht über den Verschlüsselungsstatus der Massenspeichergeräte

- Bericht über Zugriffsrechte auf verschlüsselte Laufwerke

- Bericht über Fehler bei der Dateiverschlüsselung

*So generieren Sie einen Verschlüsselungsbericht im Abschnitt **Verschlüsselung und Datenschutz**:*

1. Stellen Sie sicher, dass Sie die Option **Verschlüsselung und Datenschutz anzeigen** in den Einstellungen der Benutzeroberfläche aktiviert haben.

2. Gehen Sie in den Eigenschaften für Richtlinien zur Registerkarte **Konfiguration von Ereignissen**.

3. Klicken Sie im Abschnitt **Kritisch** auf **Ereignis hinzufügen** und aktivieren Sie das Kontrollkästchen neben dem Ereignis *Fehler bei der Anwendung von Regeln zur Verschlüsselung / Entschlüsselung von Dateien*.

4. Klicken Sie auf die Schaltfläche **OK**.

5. Gehen Sie im Hauptmenü zu **Vorgänge → Verschlüsselung und Datenschutz**.

6. Öffnen Sie einen der folgenden Abschnitte:

   - **Verschlüsselte Laufwerke**, erstellt den Bericht über den Verschlüsselungsstatus der Massenspeichergeräte oder den Bericht über Zugriffsrechte auf verschlüsselte Laufwerke.
   - **Verschlüsselungsereignisse** erstellt den Bericht über Fehler bei der Dateiverschlüsselung.

7. Klicken Sie auf den Namen des Berichts, den Sie erstellen möchten.

Die Erstellung des Berichts wird gestartet.

Zugriff auf ein verschlüsseltes Laufwerk im autonomen Modus gewähren

Ein Benutzer kann den Zugriff auf ein verschlüsseltes Gerät anfordern, wenn beispielsweise kein Kaspersky Endpoint Security auf dem verwalteten Gerät installiert ist. Nachdem Sie die Anforderung erhalten haben, können Sie eine Datei mit einem Zugriffsschlüssel erstellen und an den Benutzer senden. Alle Anwendungsfälle und detaillierten Anweisungen finden Sie in der Hilfe zu Kaspersky Endpoint Security für die jeweilige Plattform.

So gewähren Sie in Kaspersky Endpoint Security für Windows Zugriff auf ein verschlüsseltes Laufwerk im Offline-Modus:

1. Rufen Sie eine Zugriffsanfrage-Datei von einem Benutzer ab (eine Datei mit der Erweiterung FDERTC). Folgen Sie den Anweisungen der Hilfe von Kaspersky Endpoint Security für Windows um die Datei in Kaspersky Endpoint Security für Windows zu generieren.
2. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Verschlüsselung und Datenschutz** → **Verschlüsselte Laufwerke**.
   Eine Liste mit den verschlüsselten Laufwerken wird geöffnet.
3. Wählen Sie das Laufwerk aus, für welches der Benutzer den Zugriff angefordert hat.
4. Klicken Sie auf die Schaltfläche **Zugriff auf das Gerät im autonomen Modus gewähren**.
5. Wählen Sie im folgenden Fenster das Plug-in für Kaspersky Endpoint Security für Windows aus.
6. Folgen Sie den Anweisungen in der Hilfe von Kaspersky Endpoint Security für Windows https://support.kaspersky.com/KESWin/12.12/de-DE/130941.htm (siehe Anweisungen für Kaspersky Security Center Web Console am Ende des Abschnitts).

Anschließend kann der Benutzer die empfangene Datei verwenden, um auf das verschlüsselte Laufwerk zuzugreifen und die auf dem Laufwerk gespeicherten Daten zu lesen.

Übertragung von Chiffrierschlüsseln zwischen Administrationsservern

Wenn die Datenverschlüsselungsfunktion auf einem verwalteten Gerät aktiviert ist, so ist der Chiffrierschlüssel auf dem Administrationsserver gespeichert. Der Chiffrierschlüssel wird verwendet, um auf verschlüsselte Daten zuzugreifen und um die Verschlüsselungsrichtlinie zu verwalten.

Der Chiffrierschlüssel muss in folgenden Fällen an einen anderen Administrationsserver übertragen werden:

- Wenn der Administrationsagent auf einem verwalteten Gerät neu konfiguriert wird, um das Gerät einem anderen Administrationsserver zuzuweisen. Wenn dieses Gerät verschlüsselte Daten enthält, muss der Chiffrierschlüssel an den Ziel-Administrationsserver übertragen werden. Andernfalls können die Daten nicht entschlüsselt werden.

- Wenn ein Wechseldatenträger, der mit einem vom Administrationsserver S1 verwalteten Gerät G1 verbunden ist, verschlüsselt wird und anschließend mit einem vom Administrationsserver S2 verwalteten Gerät G2 verbunden wird. Um auf die Daten des Wechseldatenträgers zugreifen zu können, muss der Chiffrierschlüssel von Administrationsserver S1 zu Administrationsserver S2 übertragen werden.

- Wenn eine Datei auf dem durch den Administrationsserver S1 verwalteten Gerät G1 verschlüsselt wird und anschließend versucht wird, die Datei auf einem durch den Administrationsserver S2 verwalteten Gerät G2 zu öffnen. Um auf die Datei zugreifen zu können, muss der Chiffrierschlüssel von Administrationsserver S1 zu Administrationsserver S2 übertragen werden.

Sie können Chiffrierschlüssel wie folgt übertragen:

- Automatisch durch Aktivieren der Option **Hierarchie der Administrationsserver benutzen, um Chiffrierschlüssel abzurufen** in den Eigenschaften von zwei Administrationsservern, zwischen denen ein Chiffrierschlüssel übertragen werden muss. Wenn diese Option für einen der Administrationsserver deaktiviert ist, so ist die automatische Übertragung von Chiffrierschlüsseln nicht möglich.

  Wenn Sie in den Einstellungen des Administrationsservers die Option **Hierarchie der Administrationsserver benutzen, um Chiffrierschlüssel abzurufen** aktivieren, sendet der Administrationsserver sämtliche, in seiner Datenverwaltung befindliche, Chiffrierschlüssel an den primären Administration Server (falls vorhanden) der nächsthöheren Hierarchie-Ebene.

  Wenn Sie versuchen, auf verschlüsselte Daten zuzugreifen, durchsucht der Administrationsserver zuerst die Chiffrierschlüssel in seiner eigenen Datenverwaltung. Wenn die Option **Hierarchie der Administrationsserver benutzen, um Chiffrierschlüssel abzurufen** aktiviert ist und der erforderliche Chiffrierschlüssel nicht in der Datenverwaltung gefunden wurde, sendet der Administrationsserver zusätzlich eine Anfrage an die primären Administrationsserver (falls vorhanden), damit der erforderliche Chiffrierschlüssel bereitgestellt wird. Die Anfrage wird an alle primären Administrationsserver bis zum Server auf der höchsten Hierarchie-Ebene gesendet.

- Manuell von einem Administrationsserver zu einem anderen durch den Export und Import einer Datei mit den Verschlüsselungsschlüsseln.

  Der Export und Import von Chiffrierschlüsseln sind Vorgänge, die in der Verwaltungsfunktion für Chiffrierschlüssel enthalten sind. Um diese Vorgänge auszuführen, Konfigurieren Sie die Zugriffsrechte auf die Funktion für Benutzer von Kaspersky Security Center Linux wie folgt:

  - Gewähren Sie für einen Benutzer, der Chiffrierschlüssel vom sekundären Administrationsserver exportiert, die Zugriffsberechtigung **Lesen** auf die Verwaltungsfunktion für Chiffrierschlüssel.

  - Gewähren Sie für einen Benutzer, der Chiffrierschlüssel in den sekundären Ziel-Administrationsserver importiert die Zugriffsberechtigung auf die Verwaltungsfunktion für Chiffrierschlüssel **Schreiben**.

Um die automatische Übertragung von Chiffrierschlüsseln zwischen Administrationsservern innerhalb der Hierarchie zu aktivieren:

1. Wechseln Sie zu den Eigenschaften des gewünschten Administrationsservers:

   a. Wählen Sie im Hauptmenü einen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**), und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

   b. Bewegen Sie im neuen Navigationsbereich den Mauszeiger über den Namen des erforderlichen Administrationsservers und klicken Sie anschließend auf das Einstellungssymbol (⚙).

      Alternativ können Sie auf den Namen des Administrationsservers klicken und wenn der Name anschließend im Hauptmenü angezeigt wird, auf diesen klicken, um das Eigenschaftsfenster des Servers zu öffnen.

2. Wählen Sie im daraufhin neuen Eigenschaftsfenster den Abschnitt **Verschlüsselungsalgorithmus** aus.

3. Aktivieren Sie die Option **Hierarchie der Administrationsserver benutzen, um Chiffrierschlüssel abzurufen**.

4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu übernehmen.

Die Chiffrierschlüssel werden bei der nächsten Synchronisierung (Heartbeat) an die primären Administrationsserver (falls vorhanden) übertragen. Dieser Administrationsserver stellt auch auf Anfrage einen Chiffrierschlüssel aus seiner Datenverwaltung für einen sekundären Administrationsserver bereit.

Um die Chiffrierschlüssel manuell zwischen Administrationsservern zu übertragen:

1. Wechseln Sie zu den Eigenschaften des Administrationsservers, von dem Sie Chiffrierschlüssel exportieren möchten:

   a. Wählen Sie im Hauptmenü einen Abschnitt aus (mit Ausnahme von **Marketplace**, **Konsolen-Navigation** und **Einstellungen**), und klicken Sie anschließend im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.

   b. Bewegen Sie im neuen Navigationsbereich den Mauszeiger über den Namen des erforderlichen Administrationsservers und klicken Sie anschließend auf das Einstellungssymbol (⚙).

      Alternativ können Sie auf den Namen des Administrationsservers klicken und wenn der Name anschließend im Hauptmenü angezeigt wird, auf diesen klicken, um das Eigenschaftsfenster des Servers zu öffnen.

2. Wählen Sie im daraufhin neuen Eigenschaftsfenster den Abschnitt **Verschlüsselungsalgorithmus** aus.

3. Klicken Sie auf **Chiffrierschlüssel von Administrationsserver exportieren**.

   Stellen Sie sicher, dass einem Benutzer, der Chiffrierschlüssel vom Server exportiert, die Zugriffsberechtigung auf die Verwaltungsfunktion für Chiffrierschlüssel **Lesen** gewährt wurde.

4. Im Fenster **Chiffrierschlüssel exportieren**:

   - Klicken Sie auf **Durchsuchen** und geben Sie dann an, wo die Datei gespeichert werden soll.
   - Geben Sie ein Kennwort an, um die Datei vor unbefugtem Zugriff zu schützen.

     Merken Sie sich das Kennwort. Ein verlorenes Kennwort kann nicht wiederhergestellt werden. Wenn das Kennwort verloren geht, müssen Sie den Exportvorgang wiederholen. Notieren Sie sich daher das Kennwort und habe Sie es griffbereit.

5. Übertragen Sie die Datei auf einen anderen Administrationsserver, z. B. über einen freigegebenen Ordner oder einen Wechseldatenträger.

6. Wechseln Sie zu den Eigenschaften des Administrationsservers, auf den Sie die Chiffrierschlüssel importieren möchten.

7. Wählen Sie im Eigenschaftenfenster den Abschnitt **Verschlüsselungsalgorithmus** aus.

8. Klicken Sie auf die Schaltfläche **Chiffrierschlüssel in Administrationsserver importieren**.

   Stellen Sie sicher, dass einem Benutzer, der Chiffrierschlüssel auf einem Server importiert, die Zugriffsberechtigung **Schreiben** auf die Verwaltungsfunktion für Chiffrierschlüssel gewährt wurde.

9. Im Fenster **Importiere Chiffrierschlüssel**:

   - Klicken Sie auf **Durchsuchen** und wählen Sie dann die Datei mit den Chiffrierschlüsseln aus.
   - Geben Sie das Kennwort an.

10. Klicken Sie auf die Schaltfläche **OK**.

Die Chiffrierschlüssel werden an den Zieladministrationsserver übertragen.

Administrationsserver für Client-Geräte wechseln

Sie können für bestimmte Client-Geräte einen anderen Administrationsserver festlegen. Verwenden Sie dazu die Aufgabe *Administrationsserver wechseln*.

Um einen Administrationsserver, der die Client-Geräte verwaltet, zu wechseln, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die Geräte verwaltet.

2. Erstellen Sie die Aufgabe "Administrationsserver ändern".

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten. Wählen Sie im Fenster **Neue Aufgabe** des Assistenten für das Erstellen einer Aufgabe die Anwendung **Kaspersky Security Center 16.3** und den Aufgabentyp **Administrationsserver wechseln** aus. Geben Sie dann die Geräte an, für die Sie den Administrationsserver ändern möchten:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

   - **Geräteadressen manuell angeben oder aus Liste importieren**

     Sie können DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die Aufgabe zugewiesen werden soll.

Diese Option können Sie beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

3. Starten Sie die erstellte Aufgabe.

Nach Abschluss der Aufgabe werden die Client-Geräte, für welche die Aufgabe erstellt wurde, auf den Administrationsserver umgestellt, der in den Einstellungen der Aufgabe angegeben wurde.

Wenn der Administrationsserver Verschlüsselung und Datenschutz unterstützt und Sie eine Aufgabe *Administrationsserver wechseln* erstellen, wird eine Warnung angezeigt. Die Warnung besagt, dass für den Fall, dass verschlüsselte Daten auf Geräten gespeichert werden, nachdem der neue Server mit der Verwaltung der Geräte beginnt, Benutzer nur auf die verschlüsselten Daten zugreifen können, mit denen sie zuvor gearbeitet haben. In anderen Fällen werden die Daten nicht freigegeben. Eine ausführliche Beschreibung der Fälle, in denen die verschlüsselten Daten nicht freigegeben werden, können Sie der Hilfe von Kaspersky Endpoint Security für Windows entnehmen.

Konflikte zwischen mehreren Administrationsservern vermeiden

Wenn Sie mehr als einen Administrationsserver in Ihrem Netzwerk verwenden, können diese dieselben Client-Geräte sehen. Dies kann Konflikten führen, wenn etwa ein Administrationsserver eine Anwendung installiert, die bereits von einem anderen Administrationsserver installiert wurde. Um zu verhindern, dass eine Anwendung auf einem Gerät installiert wird, das durch einen anderen Administrationsserver verwaltet wird, müssen Sie in den Eigenschaften der Aufgabe *Remote-Installation einer Anwendung* die Option **Nur auf Geräten installieren, die durch diesen Administrationsserver verwaltet werden** aktivieren.

Wenn Sie die Option **Nur auf Geräten installieren, die durch diesen Administrationsserver verwaltet werden** aktivieren und anschließend die Aufgabe *Remote-Installation einer Anwendung* ausführen, findet eine Prüfung statt, ob die Geräte von einem anderen Administrationsserver verwaltet werden. Für verwaltete Geräte, die durch einen anderen Administrationsserver verwaltet werden, wird der Wert des Attributs **Verwaltung erfolgt durch anderen Administrationsserver** auf `true` gesetzt. Die Aufgabe *Remote-Installation einer Anwendung* wird auf diese Geräte nicht angewendet.

Der Wert des Attributs **Verwaltung erfolgt durch anderen Administrationsserver** wird in der Spalte **Verwaltung erfolgt durch anderen Administrationsserver** der Liste der verwalteten Geräte und der Liste der nicht zugewiesenen Geräte angezeigt.

Sie können die Eigenschaft **Verwaltung erfolgt durch anderen Administrationsserver** auch als Kriterium für folgende Zwecke verwenden:

- Anzeigen verwalteter Geräte
- Geräteauswahlen

- Verschiebungsregeln für Geräte
- Regeln für die automatische Tag-Zuweisung

Um das Attribut Verwaltung erfolgt durch anderen Administrationsserver zurückzusetzen:

1. Wechseln Sie im Hauptmenü von Kaspersky Security Center Web Console zu **Asset-Verwaltung → Nicht zugeordnete Geräte**.
2. Wählen Sie das gewünschte Gerät aus und klicken Sie anschließend auf die Schaltfläche **Attribut "Verwaltung erfolgt durch anderen Administrationsserver" entfernen**.

Das Attribut **Verwaltung erfolgt durch anderen Administrationsserver** wird zurückgesetzt.

Geräte, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind, auf einen anderen Administrationsserver verschieben

Sie können Geräte, die über Verbindungs-Gateways mit dem Administrationsserver verbunden sind, auf einen anderen Administrationsserver verschieben. Dies kann beispielsweise erforderlich sein, wenn Sie eine andere Version des Administrationsservers installieren und dabei den Administrationsagenten auf den Geräten nicht erneut installieren möchten, um Zeit zu sparen.

Die in dieser Anleitung beschriebenen Befehle müssen auf Client-Geräten unter einem Benutzerkonto mit Administratorrechten ausgeführt werden.

So verschieben Sie ein Gerät, das über das Verbindungs-Gateway verbunden ist, auf einen anderen Administrationsserver:

1. Starten Sie das Tool klmover mit dem Parameter `-address < Serveradresse >`, um zu dem neuen Administrationsserver zu wechseln.
2. Führen Sie den Befehl `klnagchk -nagwait -tl 4` aus.
3. Führen Sie die folgenden Befehle aus, um ein neues Verbindungs-Gateway anzugeben:
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "< IP oder Name des Gateways >" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `<IP oder Name des Gateways >` entspricht hier der Adresse des Verbindungs-Gateways, mit der über das Internet auf das Gateway zugegriffen werden kann.

- `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

  `13000` steht für die Nummer des TCP-Ports, der das Verbindungs-Gateway überwacht.

4. Führen Sie den Befehl `klnagchk -restart -tl 4` aus, um den Dienst des Administrationsagenten zu starten.

Das Gerät wird auf den neuen Administrationsserver verschoben und über das neue verbundene Gateway verbunden.

Maßnahmen anzeigen und konfigurieren, wenn Geräte als inaktiv angezeigt werden

Wenn Client-Geräte innerhalb einer Gruppe inaktiv sind, können Sie Benachrichtigungen darüber erhalten. Sie können solche Geräte auch automatisch löschen.

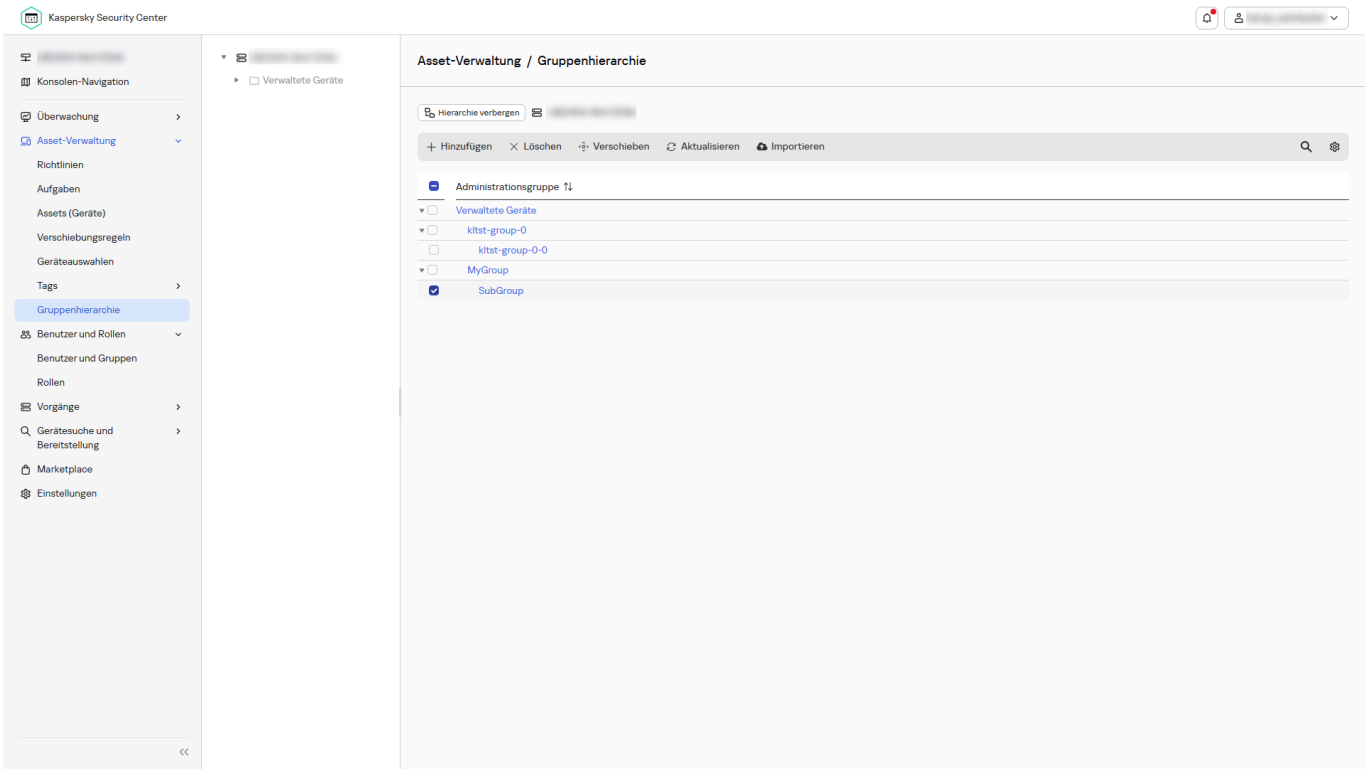
Um die Aktionen bei inaktiven Geräten innerhalb einer Gruppe anzuzeigen oder anzupassen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Gruppenhierarchie**.

2. Wechseln Sie auf eine der folgenden Arten zu den Eigenschaften der erforderlichen Administrationsgruppe:

   - Klicken Sie auf den Namen der Administrationsgruppe.

   - Klicken Sie im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**. Bewegen Sie im neuen Navigationsbereich den Mauszeiger über den Namen der gewünschten Gruppe und klicken Sie anschließend auf das Einstellungssymbol (⚙).



Eine Hierarchie von Administrationsgruppen

Das Eigenschaftenfenster der übergeordneten Administrationsgruppe wird geöffnet.

3. Gehen Sie im Eigenschaftenfenster zur Registerkarte **Einstellungen**.

4. Aktivieren oder deaktivieren Sie im Abschnitt **Vererbung** die folgenden Optionen:

- **Aus übergeordneter Gruppe erben**

  Die Einstellungen in diesem Abschnitt werden von der übergeordneten Gruppe geerbt, in der das Client-Gerät enthalten ist. Wenn diese Option aktiviert ist, sind die Einstellungen unter **Geräteaktivität im Netzwerk** für alle Änderungen gesperrt.

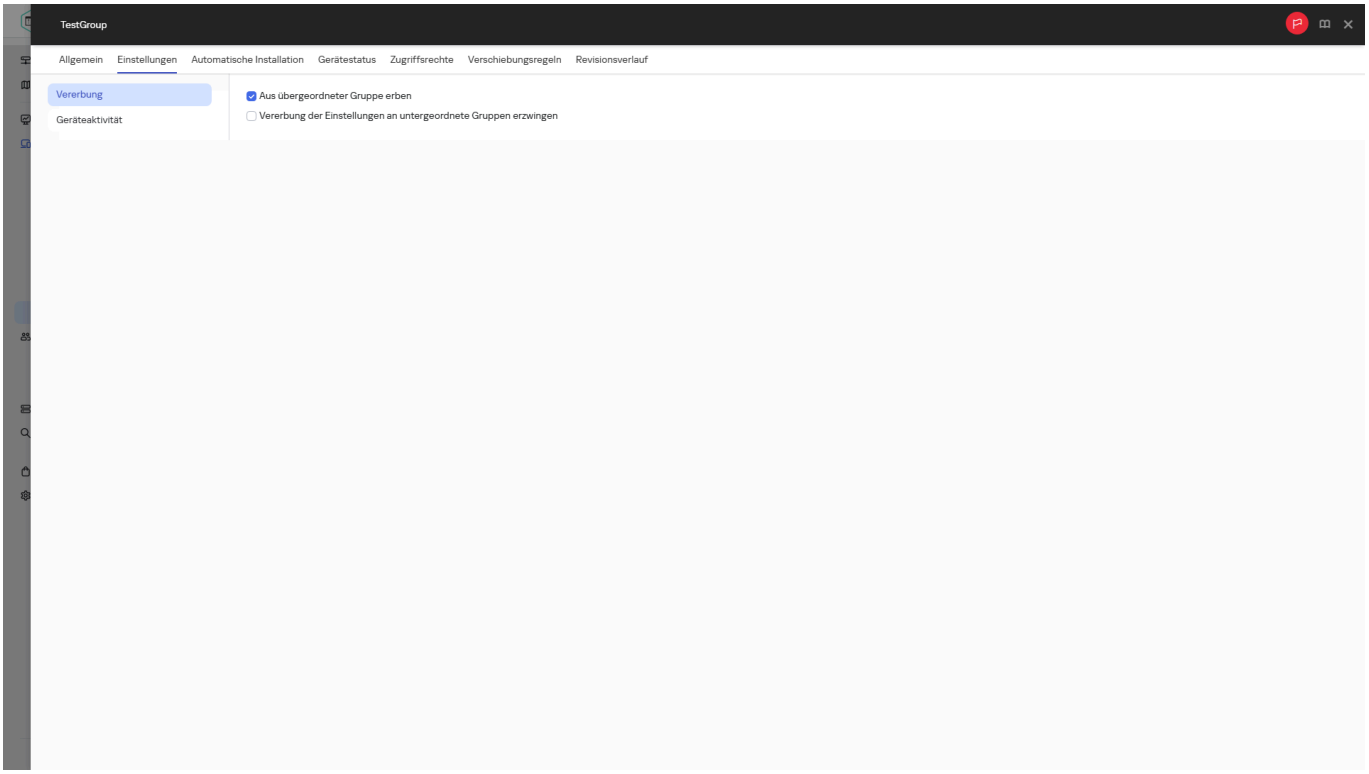
  Diese Option ist nur verfügbar, wenn die Administrationsgruppe über eine übergeordnete Gruppe verfügt.

  Diese Option ist standardmäßig aktiviert.

- **Vererbung der Einstellungen an untergeordnete Gruppen erzwingen**

  Die Einstellungswerte werden an untergeordnete Gruppen verteilt, aber in den Eigenschaften der untergeordneten Gruppen sind diese Einstellungen gesperrt.

  Diese Option ist standardmäßig deaktiviert.



Eigenschaften einer Administrationsgruppe

5. Aktivieren oder deaktivieren Sie im Abschnitt **Geräteaktivität** die folgenden Optionen:

- **Administrator benachrichtigen, wenn Gerät inaktiv seit (Tagen)**

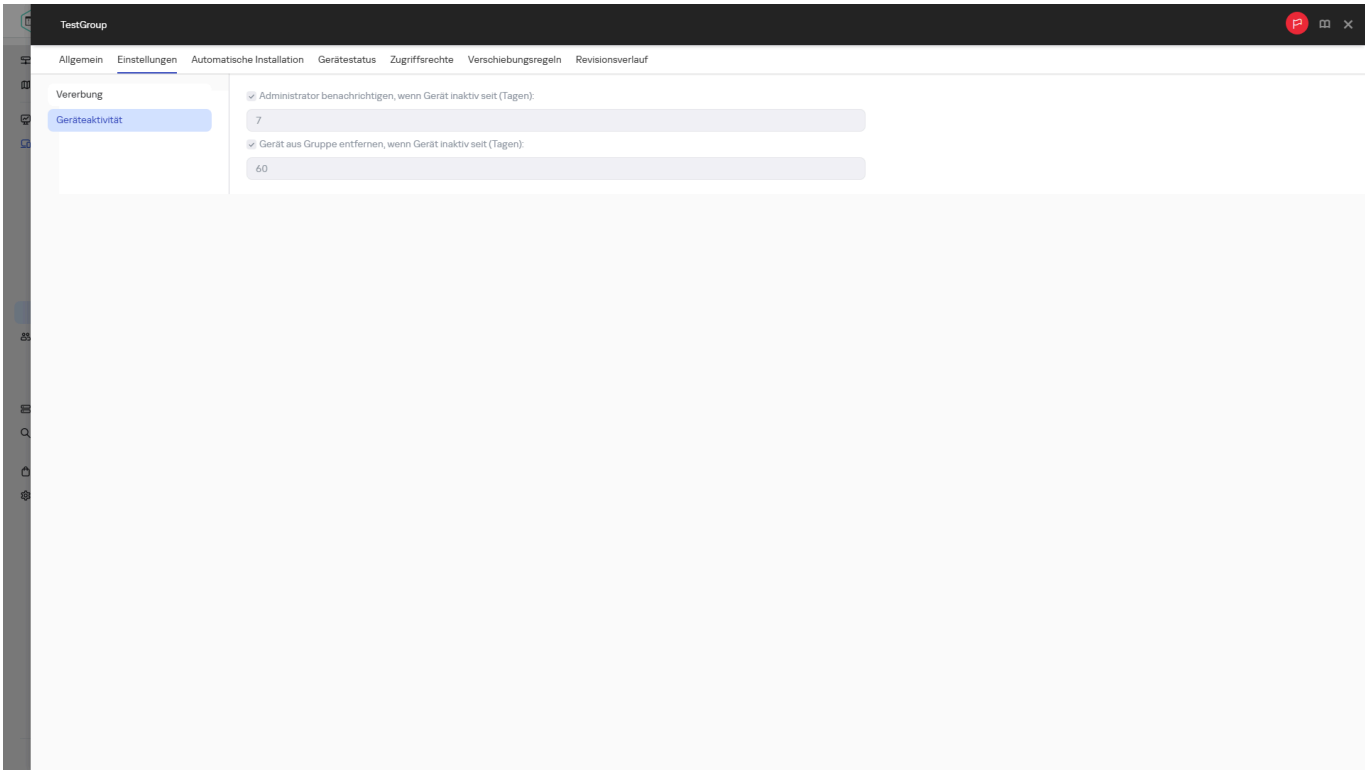
  Wenn diese Option aktiviert ist, erhält der Administrator Benachrichtigungen über inaktive Geräte. Sie können das Zeitintervall angeben, nach dem das Ereignis **Gerät zu lange inaktiv im Netzwerk** erstellt wird. Standardmäßig beträgt das Zeitintervall 7 Tage.

  Diese Option ist standardmäßig aktiviert.

- **Gerät aus Gruppe entfernen, wenn Gerät inaktiv seit (Tagen)**

  Wenn diese Option aktiviert ist, können Sie das Zeitintervall festlegen, nach dem das Geräte automatisch aus der Gruppe gelöscht wird. Standardmäßig beträgt das Zeitintervall 60 Tage.

Diese Option ist standardmäßig aktiviert.



Eigenschaften einer Administrationsgruppe

6. Klicken Sie auf die Schaltfläche **Speichern**.

Ihre Änderungen werden gespeichert und übernommen.

Nachricht an Gerätenutzer senden

Um eine Nachricht an Gerätenutzer zu senden, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Nachricht an Benutzer**.
4. Wählen Sie eine Option, um die Administrationsgruppe, die Geräteauswahl oder die Geräte, für die Aufgabe gilt, festzulegen.
5. Starten Sie die erstellte Aufgabe.

Nach Abschluss der Aufgabe wird die Nachricht an die Benutzer der gewählten Geräte gesendet. Die Aufgabe **Nachricht an Benutzer** ist nur für Geräte verfügbar, die unter Windows laufen.

Client-Geräte von einem entfernten Standort einschalten, ausschalten und Neustart durchführen

Kaspersky Security Center Linux ermöglicht die Remoteverwaltung (Einschalten, Ausschalten und Neustarten) von Client-Geräten.

Um Client-Geräte im Remote-Betrieb zu verwalten, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Verwaltung der Geräte**.
4. Wählen Sie eine Option, um die Administrationsgruppe, die Geräteauswahl oder die Geräte, für die Aufgabe gilt, festzulegen.
5. Wählen Sie den Befehl aus (einschalten, Herunterfahren oder neu starten).
6. Passen Sie bei Bedarf die folgenden Einstellungen für die Befehle zum Herunterfahren oder Neu starten an:

   - Aktivieren Sie den Schalter **Bestätigung durch Benutzer einholen**, um die Nachricht für eine Benutzeraufforderung einzugeben und die Zeitintervalle festzulegen, in denen die Aufforderung wiederholt werden soll und die Geräte Neu starten oder ausgeschaltet werden sollen.
   - Aktivieren Sie das Kontrollkästchen **Erzwungenes Schließen von Anwendungen in gesperrten Sitzungen nach (Min.)** und geben Sie die Dauer ein.

   Diese Einstellungen Anwendung für Client-Geräte unter Windows. Linux-Geräte werden unmittelbar nach dem, Abschluss der Aufgabe Neu starten oder Herunterfahren.
7. Starten Sie die erstellte Aufgabe.

Nach Abschluss der Aufgabe wird der Befehl (Einschalten, Ausschalten oder Neu starten) auf den ausgewählten Geräten ausgeführt.

Remote-Zugriff auf verwaltete Geräte

Mit Kaspersky Security Center Linux können Sie eine Remote-Verbindung zu verwalteten Geräten herstellen. Der Administrator kann Remote-Zugriff auf das verwaltete Gerät mithilfe des Administrationsagenten bekommen, der auf dem Client-Gerät installiert wurde. Die Remoteverbindung mit dem Client-Gerät mithilfe des Administrationsagenten ist sogar dann möglich, wenn die TCP- und UDP-Ports des Client-Geräts geschlossen sind. Nach der Verbindung mit dem Gerät bekommt der Administrator vollständigen Zugriff auf die Informationen dieses Geräts und kann die auf diesem Gerät installierten Programme verwalten.

Die Methoden zum Herstellen einer Remote-Verbindung hängen davon ab, welche Plattform das Gerät mit Kaspersky Security Center Web Console verwendet. Die Kaspersky Security Center Web Console kann auf einem anderen Windows- oder Linux-basierten Gerät installiert werden als auf dem Gerät des Administrationsservers.

Wenn Kaspersky Security Center Web Console auf einem Linux-Gerät installiert ist, können Sie die folgenden Verbindungen herstellen:

- Zu einem Linux-basierten verwalteten Gerät mithilfe von:
  - Remotedesktopverbindung (RDP)
  - Virtual Network Computing (VNC)
- Zu einem Windows-basierten verwalteten Gerät mithilfe von:
  - Remotedesktopverbindung (RDP)
  - Virtual Network Computing (VNC)

Wenn Kaspersky Security Center Web Console auf einem Windows-Gerät installiert ist, können Sie die folgenden Verbindungen herstellen:

- Zu einem Linux-basierten verwalteten Gerät mithilfe von:
  - Remotedesktopverbindung (RDP)
  - Virtual Network Computing (VNC)
- Zu einem Windows-basierten verwalteten Gerät mithilfe von:
  - Remotedesktopverbindung (RDP)
  - Windows Desktopfreigabe (WDS)

Wenn Sie von einem Gerät mit Microsoft Windows on Arm auf die Kaspersky Security Center Web Console zugreifen, sind keine Remote-Verbindungen mit verwalteten Geräten möglich.

Um eine Remoteverbindung mit einem Gerät herzustellen, wird Folgendes benötigt:

- Tool "klsctunnel"

  Das Kaspersky-Tool wird zum Tunneln der Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver verwendet.

  Kaspersky Security Center Linux erlaubt das Tunneln der TCP-Verbindungen von der Kaspersky Security Center Web Console über den Administrationsserver und weiter über den Administrationsagenten zum angegebene Port auf dem verwalteten Gerät. Wenn keine direkte Verbindung zwischen der Kaspersky Security Center Web Console und dem verwalteten Gerät möglich ist, wird der Tunnel zum Verbinden eines Client-Programms auf einem Gerät mit installierter Kaspersky Security Center Web Console zum TCP-Port eines verwalteten Geräts verwendet.

Es ist erforderlich, die Verbindung eines Remote-Client-Geräts mit dem Administrationsserver zu tunneln, wenn der Port für die Verbindung mit dem Administrationsserver auf dem Gerät nicht verfügbar ist. Der Port auf dem Gerät kann in folgenden Fällen nicht verfügbar sein:

- Das Remote-Gerät ist mit einem lokalen Netzwerk verbunden, in dem das NAT-Verfahren verwendet wird.
- Das Remote-Gerät gehört zum lokalen Netzwerk des Administrationsservers, sein Port wird jedoch von der Firewall geschlossen.

Das Tool kann entweder über eine Remote-Verbindung durch die Kaspersky Security Center Web Console oder manuell von der Kaspersky-Website heruntergeladen werden.

Das Tool "klsctunnel" ist auf dem Gerät mit dem Administrationsserver installiert und wird zur Herstellung von Remote-Verbindungen aller Art (RDP, VNC, WDS) verwendet.

- RDP- oder VNC-Client

  Auf dem Gerät des Administrationsservers ist ein RDP oder VNC-Client installiert. Mit diesem Client können Sie Remote-Zugriff auf ein verwaltetes Gerät erhalten, indem Sie die vom Tool "klsctunnel" bereitgestellte Adresse und den Port für die lokale Verbindung verwenden.

  Eine RDP-Verbindung zu der aktuellen Sitzung des Remotedesktops des Benutzers wird ohne Benachrichtigung des Benutzers hergestellt. Sobald sich der Administrator mit der Sitzung verbunden hat, wird der Benutzer des Client-Geräts ohne Benachrichtigung von der Sitzung abgemeldet.

- Windows Desktopfreigabe (nur für Windows-basierte verwaltete Geräte)

  Mit dieser Funktionen können Sie eine Verbindung zu einer vorhandenen Sitzung auf dem Client-Gerät herstellen, ohne dass der Benutzer dieser Sitzung getrennt wird. In diesem Fall haben der Administrator und der Benutzer der Sitzung auf dem Gerät einen gemeinsamen Zugriff auf den Desktop.

  Bei der Verbindung mit einer vorhandenen Remotedesktop-Sitzung empfängt der Benutzer der Sitzung auf dem Gerät eine Anfrage zum Herstellen der Verbindung vom Administrator. In den von Kaspersky Security Center Linux erstellten Berichten werden keinerlei Informationen über die Remote-Aktivitäten und deren Ergebnisse gespeichert.

  Der Administrator kann ein Audit der Aktionen auf dem Remote-Client-Gerät konfigurieren. Während des Audits werden Informationen über die Dateien auf dem Client-Gerät gesammelt, die vom Administrator geöffnet bzw. geändert werden.

Remote-Zugriff von einem Linux-basierten Gerät mit Kaspersky Security Center Web Console auf ein verwaltetes Linux-Gerät

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass:

- auf dem verwalteten Linux-Gerät der Administrationsagent in Version 15.3 oder höher installiert ist.
- auf dem verwalteten Gerät unter Linux ist der RDP-Server installiert ist (wenn Sie sich per Remote Desktop Connection mit dem verwalteten Gerät verbinden).
- auf dem verwalteten Gerät unter Linux ist der VNC-Server installiert ist (wenn Sie sich per Virtual Network Computing mit dem verwalteten Gerät verbinden).

- der Port zum Tunneln von RDP-Verbindungen geöffnet ist (die Option **Port zum Tunneln der RDP-Verbindungen öffnen** ist im Abschnitt **Verbindungsports** des Eigenschaftsfensters des Administrationsservers aktiviert).

- der Administrator über das Recht **RDP-Sitzungen starten** verfügt, um RDP-Verbindungen herzustellen (wenn Sie sich per Remotedesktopverbindung mit dem verwalteten Gerät verbinden).

- der Administrator über das Recht **Tunnelung starten** verfügt, um Tunnel-Verbindungen für VNC herzustellen (wenn Sie sich per Virtual Network Computing mit dem verwalteten Gerät verbinden).

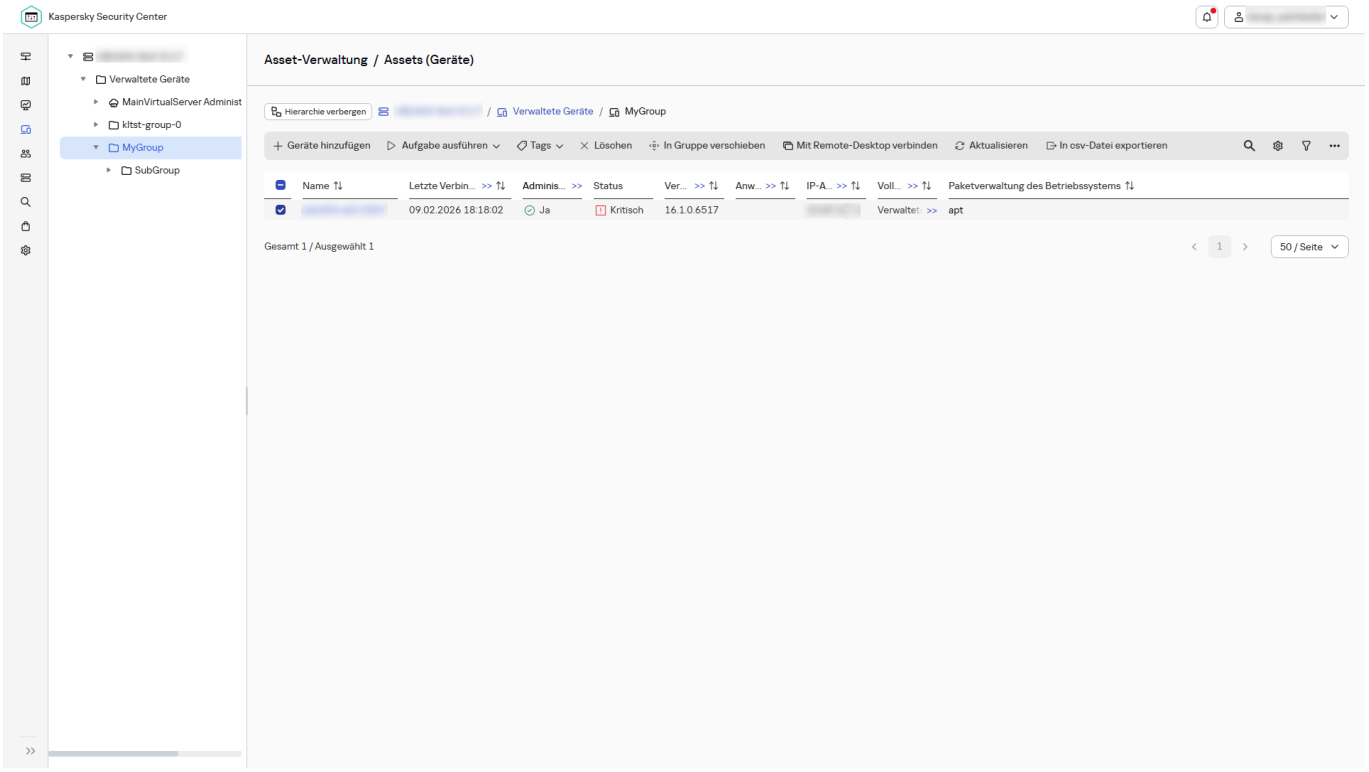
Gehen Sie wie folgt vor, um mithilfe von RDP oder VNC über die auf einem Linux-Gerät geöffnete Kaspersky Security Center Web Console eine Verbindung mit einem verwalteten Linux-Gerät herzustellen:

1. Navigieren Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung → Assets (Geräte)** oder öffnen Sie eine Geräteauswahl.

2. Aktivieren Sie das Kontrollkästchen neben dem verwalteten Gerät, mit dem Sie eine Remote-Verbindung herstellen möchten, und klicken Sie anschließend auf die Schaltfläche **Mit Remote-Desktop verbinden**.

   Das Fenster **Mit Remote-Desktop verbinden** wird geöffnet.

   Wenn Sie mehrere Geräte, ein Mobilgerät oder ein Gerät mit macOS auswählen, wird die Schaltfläche **Mit Remote-Desktop verbinden** deaktiviert.



Die Liste der verwalteten Geräte

3. Laden Sie das Tool "klsctunnel" herunter, indem Sie auf die Schaltfläche **Download** klicken, und führen Sie es anschließend aus.

Folgendes sollten Sie beim Download des Tools beachten:

- Um eine aktuelle Version des Tools "klsctunnel" zu erhalten, stellen Sie sicher, dass der Administrationsserver auf die Kaspersky-Update-Server zugreifen kann.

  Sie können die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausführen und als Update-Quelle die Kaspersky-Update-Server auswählen. Wenn die Aufgabe erfolgreich abgeschlossen wird, hat der Administrationsserver Zugriff auf die Kaspersky-Update-Server.

- Wenn das Tool nicht zum Download verfügbar ist, wird eine Fehlermeldung angezeigt. In diesem Fall können Sie das Tool manuell herunterladen und es anschließend auf dem Gerät mit dem Administrationsserver im Verzeichnis "/var/opt/kaspersky/klnagent_srv" platzieren.

4. Geben Sie im Fenster **Mit Remote-Desktop verbinden** den Verbindungsport an. Standardmäßig ist die Portnummer 3389 festgelegt.

5. Generieren Sie ein Text-BLOB mit codierten Verbindungsparametern, indem Sie auf die Schaltfläche **BLOB generieren** klicken und den Text anschließend kopieren und in das entsprechende Feld des Tools "klsctunnel" einfügen.

   Ein Blob enthält die Einstellungen, die zum Herstellen einer Verbindung zwischen dem Administrationsserver und dem verwalteten Gerät erforderlich sind. Ein BLOB ist 3 Minuten lang gültig. Erzeugen Sie ein neues BLOB, wenn es abgelaufen ist.

6. Wenn Sie einen Proxyserver verwenden, geben Sie im Tool "klsctunnel" die Verbindungseinstellungen des Proxyservers an.

   Das Tool "klsctunnel" zeigt die Adresse und den Port für die lokale Verbindung eines Clients für den Remote-Zugriff an.

   Das Tool ermöglicht dem Administrator, die Tunnelverbindung zu schließen. Bei einem Schließen der Tunnelverbindung wird die aktuelle Verbindung zum Remote-Desktop beendet.

7. Führen Sie einen Remote-Access-Client (RDP oder VNC) aus und verbinden Sie ihn mit dem verwalteten Gerät, indem Sie die vom Tool "klsctunnel" bereitgestellte Adresse und den Port verwenden.

Die Verbindung zum verwalteten Gerät wird hergestellt und der Desktop ist im Fenster des Remote-Access-Clients verfügbar.

Remote-Zugriff von einem Linux-basierten Gerät mit Kaspersky Security Center Web Console auf ein verwaltetes Windows-Gerät

Remotedesktopverbindung (RDP)

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass:

- die Remoteverbindung in den Betriebssystemeinstellungen des verwalteten Zielgeräts erlaubt ist.
- auf dem verwalteten Windows-Gerät der Administrationsagent in Version 13.0 oder höher installiert ist.

- der Administrator über das Recht **RDP-Sitzungen starten** verfügt, um RDP-Verbindungen herzustellen.
- der Port zum Tunneln von RDP-Verbindungen geöffnet ist (die Option **Port zum Tunneln der RDP-Verbindungen öffnen** ist im Abschnitt **Verbindungsports** des Eigenschaftsfensters des Administrationsservers aktiviert).

Gehen Sie wie folgt vor, um mithilfe von RDP über die Kaspersky Security Center Web Console, die auf einem Linux-Gerät geöffnet ist, eine Verbindung mit einem verwalteten Windows-Gerät herzustellen:

1. Navigieren Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung** → **Assets (Geräte)** oder öffnen Sie eine Geräteauswahl.
2. Aktivieren Sie das Kontrollkästchen neben dem verwalteten Gerät, mit dem Sie eine Remote-Verbindung herstellen möchten, und klicken Sie anschließend auf die Schaltfläche **Mit Remote-Desktop verbinden**.

   Das Fenster **Mit Remote-Desktop verbinden** wird geöffnet.

   Wenn Sie mehrere Geräte, ein Mobilgerät oder ein Gerät mit macOS auswählen, wird die Schaltfläche **Mit Remote-Desktop verbinden** deaktiviert.
3. Wählen Sie im Fenster **Mit Remote-Desktop verbinden** den Verbindungstyp **RDP**.
4. Wenn die Remote-Verbindung in den Betriebssystemeinstellungen des verwalteten Geräts nicht zulässig ist, gewähren Sie zentrale Remote-Verbindungen, indem Sie auf die Schaltfläche **Einstellungen ändern** klicken.

   Wenn die Einstellungen korrekt übernommen wurden, wird eine Benachrichtigung angezeigt. Außerdem ist auf dem verwalteten Gerät im Abschnitt **Einstellungen** → **System** → **Remotedesktop** die Option **Remotedesktop aktivieren** aktiviert.

   Wenn die Remote-Verbindung in den Betriebssystemeinstellungen des verwalteten Geräts zugelassen ist, wird die Schaltfläche **Einstellungen ändern** nicht angezeigt.
5. Laden Sie das Tool "klsctunnel" herunter, indem Sie auf die Schaltfläche **Download** klicken, und führen Sie es anschließend aus.

   Folgendes sollten Sie beim Download des Tools beachten:

   - Um eine aktuelle Version des Tools "klsctunnel" zu erhalten, stellen Sie sicher, dass der Administrationsserver auf die Kaspersky-Update-Server zugreifen kann.

     Sie können die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausführen und als Update-Quelle die Kaspersky-Update-Server auswählen. Wenn die Aufgabe erfolgreich abgeschlossen wird, hat der Administrationsserver Zugriff auf die Kaspersky-Update-Server.
   - Wenn das Tool nicht zum Download verfügbar ist, wird eine Fehlermeldung angezeigt. In diesem Fall können Sie das Tool manuell herunterladen und es anschließend auf dem Gerät mit dem Administrationsserver im Verzeichnis "/var/opt/kaspersky/klnagent_srv" platzieren.
6. Generieren Sie ein Text-BLOB mit codierten Verbindungsparametern, indem Sie auf die Schaltfläche **BLOB generieren** klicken und den Text anschließend kopieren und in das entsprechende Feld des Tools "klsctunnel" einfügen.

   Ein Blob enthält die Einstellungen, die zum Herstellen einer Verbindung zwischen dem Administrationsserver und dem verwalteten Gerät erforderlich sind. Ein BLOB ist 3 Minuten lang gültig. Erzeugen Sie ein neues BLOB, wenn es abgelaufen ist.
7. Wenn Sie einen Proxyserver verwenden, geben Sie im Tool "klsctunnel" die Verbindungseinstellungen des Proxyservers an.

   Das Tool "klsctunnel" zeigt die Adresse und den Port der Verbindung zum Remote-Gerät an.

Das Tool ermöglicht dem Administrator, die Tunnelverbindung zu schließen. Bei einem Schließen der Tunnelverbindung wird die aktuelle Verbindung zum Remote-Desktop beendet.

8. Führen Sie einen RDP-Client aus und verbinden Sie ihn mit dem verwalteten Gerät, indem Sie die vom Tool "klsctunnel" bereitgestellte Adresse und den Port verwenden.

Die Verbindung zum verwalteten Gerät wird hergestellt und der Desktop ist im Fenster des RDP-Clients verfügbar.

Die Verbindung zu einer bestehenden Sitzung des Remotedesktops des Benutzers wird ohne Benachrichtigung des Benutzers hergestellt. Sobald sich der Administrator mit der Sitzung verbunden hat, wird der Benutzer des Client-Geräts ohne Benachrichtigung von der Sitzung abgemeldet.

Virtual Network Computing (VNC)

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass:

- auf dem verwalteten Windows-Gerät der Administrationsagent in Version 13.0 oder höher installiert ist.
- auf dem verwalteten Windows-Gerät der VNC-Server installiert ist.
- der Administrator über das Recht **Tunnelung starten** verfügt, um die Tunnelverbindung für VNC herzustellen.
- der Port zum Tunneln von RDP-Verbindungen geöffnet ist (die Option **Port zum Tunneln der RDP-Verbindungen öffnen** ist im Abschnitt **Verbindungsports** des Eigenschaftsfensters des Administrationsservers aktiviert).

Gehen Sie wie folgt vor, um mithilfe von VNC über die Kaspersky Security Center Web Console, die auf einem Linux-Gerät geöffnet ist, eine Verbindung zu einem verwalteten Windows-Gerät herzustellen:

1. Navigieren Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung** → **Assets (Geräte)** oder öffnen Sie eine Geräteauswahl.
2. Aktivieren Sie das Kontrollkästchen neben dem verwalteten Gerät, mit dem Sie eine Remote-Verbindung herstellen möchten, und klicken Sie anschließend auf die Schaltfläche **Mit Remote-Desktop verbinden**.

   Das Fenster **Mit Remote-Desktop verbinden** wird geöffnet.

   Wenn Sie mehrere Geräte, ein Mobilgerät oder ein Gerät mit macOS auswählen, wird die Schaltfläche **Mit Remote-Desktop verbinden** deaktiviert.
3. Wählen Sie im Fenster **Mit Remote-Desktop verbinden** den Verbindungstyp **VNC**.
4. Laden Sie das Tool "klsctunnel" herunter, indem Sie auf die Schaltfläche **Download** klicken, und führen Sie es anschließend aus.

   Wenn das Tool nicht zum Download verfügbar ist, wird eine Fehlermeldung angezeigt. Laden Sie das Tool in diesem Fall manuell herunter.
5. Geben Sie im Fenster **Mit Remote-Desktop verbinden** den VNC-Verbindungsport an. Standardmäßig ist die Portnummer 5900 festgelegt.

6. Generieren Sie ein Text-BLOB mit codierten Verbindungsparametern, indem Sie auf die Schaltfläche **BLOB generieren** klicken und den Text anschließend kopieren und in das entsprechende Feld des Tools "klsctunnel" einfügen.

   Ein Blob enthält die Einstellungen, die zum Herstellen einer Verbindung zwischen dem Administrationsserver und dem verwalteten Gerät erforderlich sind. Ein BLOB ist 3 Minuten lang gültig. Erzeugen Sie ein neues BLOB, wenn es abgelaufen ist.

7. Wenn Sie einen Proxyserver verwenden, geben Sie im Tool "klsctunnel" die Verbindungseinstellungen des Proxyservers an.

   Das Tool "klsctunnel" zeigt die Adresse und den Port für die lokale Verbindung eines VNC-Clients für den Remote-Zugriff an.

   Das Tool ermöglicht dem Remote-Benutzer, die Tunnelverbindung zu schließen. Bei einem Schließen der Tunnelverbindung wird die aktuelle Verbindung zum Remote-Desktop beendet.

8. Führen Sie einen VNC-Client aus und verbinden Sie ihn mit dem verwalteten Gerät, indem Sie die vom Tool "klsctunnel" bereitgestellte Adresse und den Port verwenden.

Die Verbindung zum verwalteten Gerät wird hergestellt und der Desktop ist im Fenster des VNC-Clients verfügbar.

Remote-Zugriff von einem Windows-basierten Gerät mit Kaspersky Security Center Web Console auf ein verwaltetes Linux-Gerät

Remotedesktopverbindung (RDP)

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass:

- auf dem verwalteten Linux-Gerät der RDP-Server installiert ist.
- auf dem verwalteten Linux-Gerät der Administrationsagent in Version 15.3 oder höher installiert ist.
- der Administrator über das Recht **RDP-Sitzungen starten** verfügt, um RDP-Verbindungen herzustellen.
- der Port zum Tunneln von RDP-Verbindungen geöffnet ist (die Option **Port zum Tunneln der RDP-Verbindungen öffnen** ist im Abschnitt **Verbindungsports** des Eigenschaftsfensters des Administrationsservers aktiviert).

Gehen Sie wie folgt vor, um mithilfe von RDP über die Kaspersky Security Center Web Console, die auf einem Windows-Gerät geöffnet ist, eine Verbindung zu einem verwalteten Linux-Gerät herzustellen:

1. Navigieren Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung** → **Assets (Geräte)** oder öffnen Sie eine Geräteauswahl.
2. Aktivieren Sie das Kontrollkästchen neben dem verwalteten Gerät, mit dem Sie eine Remote-Verbindung herstellen möchten, und klicken Sie anschließend auf die Schaltfläche **Mit Remote-Desktop verbinden**.

   Das Fenster **Mit Remote-Desktop verbinden** wird geöffnet.

Wenn Sie mehrere Geräte, ein Mobilgerät oder ein Gerät mit macOS auswählen, wird die Schaltfläche **Mit Remote-Desktop verbinden** deaktiviert.

3. Wählen Sie im Fenster **Mit Remote-Desktop verbinden** den Verbindungstyp **RDP**.

4. Laden Sie das Tool "klsctunnel" herunter, indem Sie auf die Schaltfläche **Download** klicken, und führen Sie es anschließend aus.

   Folgendes sollten Sie beim Download des Tools beachten:

   - Um eine aktuelle Version des Tools "klsctunnel" zu erhalten, stellen Sie sicher, dass der Administrationsserver auf die Kaspersky-Update-Server zugreifen kann.

     Sie können die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausführen und als Update-Quelle die Kaspersky-Update-Server auswählen. Wenn die Aufgabe erfolgreich abgeschlossen wird, hat der Administrationsserver Zugriff auf die Kaspersky-Update-Server.

   - Wenn das Tool nicht zum Download verfügbar ist, wird eine Fehlermeldung angezeigt. In diesem Fall können Sie das Tool manuell herunterladen und es anschließend auf dem Gerät mit dem Administrationsserver im Verzeichnis "/var/opt/kaspersky/klnagent_srv" platzieren.

5. Generieren Sie ein Text-BLOB mit codierten Verbindungsparametern, indem Sie auf die Schaltfläche **BLOB generieren** klicken und den Text anschließend kopieren und in das entsprechende Feld des Tools "klsctunnel" einfügen.

   Ein Blob enthält die Einstellungen, die zum Herstellen einer Verbindung zwischen dem Administrationsserver und dem verwalteten Gerät erforderlich sind. Ein BLOB ist 3 Minuten lang gültig. Erzeugen Sie ein neues BLOB, wenn es abgelaufen ist.

6. Wenn Sie einen Proxyserver verwenden, geben Sie im Tool "klsctunnel" die Verbindungseinstellungen des Proxyservers an.

   Aktivieren Sie dafür das Kontrollkästchen **Proxyserver verwenden** und geben Sie anschließend die Verbindungseinstellungen an.

7. Klicken Sie auf die Schaltfläche **Port öffnen**.

   Das Anmeldefenster für die Remotedesktopverbindung wird geöffnet.

8. Geben Sie die Anmeldeinformationen des Kontos an, mit dem Sie derzeit bei Kaspersky Security Center Web Console angemeldet sind, und verbinden Sie sich anschließend mit dem verwalteten Gerät.

   Das Tool "klsctunnel" zeigt die Adresse und den Port der Verbindung zum Remote-Gerät an.

   Das Tool ermöglicht dem Administrator, die Tunnelverbindung zu schließen. Bei einem Schließen der Tunnelverbindung wird die aktuelle Verbindung zum Remote-Desktop beendet.

Nach der Verbindung mit dem Client-Gerät ist der Desktop des Client-Geräts im Microsoft Windows-Fenster für Remoteverbindung verfügbar.

Die Verbindung zu einer bestehenden Sitzung des Remotedesktops des Benutzers wird ohne Benachrichtigung des Benutzers hergestellt. Sobald sich der Administrator mit der Sitzung verbunden hat, wird der Benutzer des Client-Geräts ohne Benachrichtigung von der Sitzung abgemeldet.

Virtual Network Computing (VNC)

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass:

- auf dem verwalteten Linux-Gerät der Administrationsagent in Version 15.3 oder höher installiert ist.
- auf dem verwalteten Linux-Gerät der VNC-Server installiert ist.
- der Administrator über das Recht **Tunnelung starten** verfügt, um die Tunnelverbindung für VNC herzustellen.
- der Port zum Tunneln von RDP-Verbindungen geöffnet ist (die Option **Port zum Tunneln der RDP-Verbindungen öffnen** ist im Abschnitt **Verbindungsports** des Eigenschaftsfensters des Administrationsservers aktiviert).

Gehen Sie wie folgt vor, um mithilfe von VNC über die Kaspersky Security Center Web Console, die auf einem Windows-Gerät geöffnet ist, eine Verbindung zu einem verwalteten Linux-Gerät herzustellen:

1. Navigieren Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung** → **Assets (Geräte)** oder öffnen Sie eine Geräteauswahl.
2. Aktivieren Sie das Kontrollkästchen neben dem verwalteten Gerät, mit dem Sie eine Remote-Verbindung herstellen möchten, und klicken Sie anschließend auf die Schaltfläche **Mit Remote-Desktop verbinden**.

   Das Fenster **Mit Remote-Desktop verbinden** wird geöffnet.

   Wenn Sie mehrere Geräte, ein Mobilgerät oder ein Gerät mit macOS auswählen, wird die Schaltfläche **Mit Remote-Desktop verbinden** deaktiviert.
3. Wählen Sie im Fenster **Mit Remote-Desktop verbinden** den Verbindungstyp **VNC**.
4. Laden Sie das Tool "klsctunnel" herunter, indem Sie auf die Schaltfläche **Download** klicken, und führen Sie es anschließend aus.

   Wenn das Tool nicht zum Download verfügbar ist, wird eine Fehlermeldung angezeigt. Laden Sie das Tool in diesem Fall manuell herunter.
5. Geben Sie im Fenster **Mit Remote-Desktop verbinden** den VNC-Verbindungsport an. Standardmäßig ist die Portnummer 5900 festgelegt.
6. Generieren Sie ein Text-BLOB mit codierten Verbindungsparametern, indem Sie auf die Schaltfläche **BLOB generieren** klicken und den Text anschließend kopieren und in das entsprechende Feld des Tools "klsctunnel" einfügen.

   Ein Blob enthält die Einstellungen, die zum Herstellen einer Verbindung zwischen dem Administrationsserver und dem verwalteten Gerät erforderlich sind. Ein BLOB ist 3 Minuten lang gültig. Erzeugen Sie ein neues BLOB, wenn es abgelaufen ist.
7. Wenn Sie einen Proxyserver verwenden, geben Sie im Tool "klsctunnel" die Verbindungseinstellungen des Proxyservers an.

   Aktivieren Sie dafür das Kontrollkästchen **Proxyserver verwenden** und geben Sie anschließend die Verbindungseinstellungen an.
8. Klicken Sie auf die Schaltfläche **Port öffnen**.

   Das Tool "klsctunnel" zeigt die Adresse und den Port für die lokale Verbindung eines VNC-Clients für den Remote-Zugriff an.

Das Tool ermöglicht dem Remote-Benutzer, die Tunnelverbindung zu schließen. Bei einem Schließen der Tunnelverbindung wird die aktuelle Verbindung zum Remote-Desktop beendet.

9. Führen Sie einen VNC-Client aus und verbinden Sie ihn mit dem verwalteten Gerät, indem Sie die vom Tool "klsctunnel" bereitgestellte Adresse und den Port verwenden.

Die Verbindung zum verwalteten Gerät wird hergestellt und der Desktop ist im Fenster des VNC-Clients verfügbar.

Remote-Zugriff von einem Windows-basierten Gerät mit Kaspersky Security Center Web Console auf ein verwaltetes Windows-Gerät

Remotedesktopverbindung (RDP)

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass:

- auf dem verwalteten Windows-Gerät der Administrationsagent in Version 13.0 oder höher installiert ist.
- der Administrator über das Recht **RDP-Sitzungen starten** verfügt, um RDP-Verbindungen herzustellen.
- der Port zum Tunneln von RDP-Verbindungen geöffnet ist (die Option **Port zum Tunneln der RDP-Verbindungen öffnen** ist im Abschnitt **Verbindungsports** des Eigenschaftsfensters des Administrationsservers aktiviert).
- die Remoteverbindung in den Betriebssystemeinstellungen des verwalteten Zielgeräts erlaubt ist.

Gehen Sie wie folgt vor, um mithilfe von RDP über die Kaspersky Security Center Web Console, die auf einem Windows-Gerät geöffnet ist, eine Verbindung mit einem verwalteten Windows-Gerät herzustellen:

1. Navigieren Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung** → **Assets (Geräte)** oder öffnen Sie eine Geräteauswahl.
2. Aktivieren Sie das Kontrollkästchen neben dem verwalteten Gerät, mit dem Sie eine Remote-Verbindung herstellen möchten, und klicken Sie anschließend auf die Schaltfläche **Mit Remote-Desktop verbinden**.

   Das Fenster **Mit Remote-Desktop verbinden** wird geöffnet.

   Wenn Sie mehrere Geräte, ein Mobilgerät oder ein Gerät mit macOS auswählen, wird die Schaltfläche **Mit Remote-Desktop verbinden** deaktiviert.
3. Wählen Sie im Fenster **Mit Remote-Desktop verbinden** den Verbindungstyp **Remote-Desktop-Verbindung**.
4. Wenn die Remote-Verbindung in den Betriebssystemeinstellungen des verwalteten Geräts nicht zulässig ist, gewähren Sie zentrale Remote-Verbindungen, indem Sie auf die Schaltfläche **Einstellungen ändern** klicken.

   Wenn die Einstellungen korrekt übernommen wurden, wird eine Benachrichtigung angezeigt. Außerdem ist auf dem verwalteten Gerät im Abschnitt **Einstellungen** → **System** → **Remotedesktop** die Option **Remotedesktop aktivieren** aktiviert.

   Wenn die Remote-Verbindung in den Betriebssystemeinstellungen des verwalteten Geräts zugelassen ist, wird die Schaltfläche **Einstellungen ändern** nicht angezeigt.

5. Laden Sie das Tool "klsctunnel" herunter, indem Sie auf die Schaltfläche **Download** klicken, und führen Sie es anschließend aus.

   Folgendes sollten Sie beim Download des Tools beachten:

   - Um eine aktuelle Version des Tools "klsctunnel" zu erhalten, stellen Sie sicher, dass der Administrationsserver auf die Kaspersky-Update-Server zugreifen kann.

     Sie können die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausführen und als Update-Quelle die Kaspersky-Update-Server auswählen. Wenn die Aufgabe erfolgreich abgeschlossen wird, hat der Administrationsserver Zugriff auf die Kaspersky-Update-Server.

   - Wenn das Tool nicht zum Download verfügbar ist, wird eine Fehlermeldung angezeigt. In diesem Fall können Sie das Tool manuell herunterladen und es anschließend auf dem Gerät mit dem Administrationsserver im Verzeichnis "/var/opt/kaspersky/klnagent_srv" platzieren.

6. Generieren Sie ein Text-BLOB mit codierten Verbindungsparametern, indem Sie auf die Schaltfläche **BLOB generieren** klicken und den Text anschließend kopieren und in das entsprechende Feld des Tools "klsctunnel" einfügen.

   Ein Blob enthält die Einstellungen, die zum Herstellen einer Verbindung zwischen dem Administrationsserver und dem verwalteten Gerät erforderlich sind. Ein BLOB ist 3 Minuten lang gültig. Erzeugen Sie ein neues BLOB, wenn es abgelaufen ist.

7. Wenn Sie einen Proxyserver verwenden, geben Sie im Tool "klsctunnel" die Verbindungseinstellungen des Proxyservers an.

   Aktivieren Sie dafür das Kontrollkästchen **Proxyserver verwenden** und geben Sie anschließend die Verbindungseinstellungen an.

8. Klicken Sie auf die Schaltfläche **Port öffnen**.

   Das Anmeldefenster für die Remotedesktopverbindung wird geöffnet.

9. Geben Sie die Anmeldeinformationen des Kontos an, mit dem Sie derzeit bei Kaspersky Security Center Web Console angemeldet sind, und verbinden Sie sich anschließend mit dem verwalteten Gerät.

   Das Tool "klsctunnel" zeigt die Adresse und den Port der Verbindung zum Remote-Gerät an.

   Das Tool ermöglicht dem Administrator, die Tunnelverbindung zu schließen. Bei einem Schließen der Tunnelverbindung wird die aktuelle Verbindung zum Remote-Desktop beendet.

Nach der Verbindung mit dem Client-Gerät ist der Desktop des Client-Geräts im Microsoft Windows-Fenster für Remoteverbindung verfügbar.

Die Verbindung zu einer bestehenden Sitzung des Remotedesktops des Benutzers wird ohne Benachrichtigung des Benutzers hergestellt. Sobald sich der Administrator mit der Sitzung verbunden hat, wird der Benutzer des Client-Geräts ohne Benachrichtigung von der Sitzung abgemeldet.

Windows Desktopfreigabe (WDS)

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass:

- auf dem verwalteten Windows-Gerät der Administrationsagent in Version 13.0 oder höher installiert ist.
- der Administrator über das Recht **Mit vorhandenen RDP-Sitzungen verbinden** verfügt, um die WDS-Verbindung herzustellen.

- die Lizenzierung für Schwachstellen- und Patch-Management verfügbar ist.
- Auf dem Administrator-Arbeitsplatz ist Microsoft Windows Vista oder höher installiert. Für die Herstellung einer Verbindung mithilfe der Windows Desktopfreigabe gibt es keine Einschränkungen hinsichtlich des Betriebssystemtyps des Geräts, auf dem der Administrationsserver installiert ist.

  Prüfen Sie, ob die Funktion für die Windows Desktopfreigabe in Ihrer Windows-Edition enthalten ist, und stellen Sie sicher, dass der Schlüssel "CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F}" in der Windows-Registry existiert.
- Microsoft Windows Vista oder höher ist auf dem Client-Gerät installiert.

Gehen Sie wie folgt vor, um mithilfe von VNC über die Kaspersky Security Center Web Console, die auf einem Windows-Gerät geöffnet ist, eine Verbindung zu einem verwalteten Windows-Gerät herzustellen:

1. Navigieren Sie im Hauptmenü zum Abschnitt **Asset-Verwaltung** → **Assets (Geräte)** oder öffnen Sie eine Geräteauswahl.
2. Aktivieren Sie das Kontrollkästchen neben dem verwalteten Gerät, mit dem Sie eine Remote-Verbindung herstellen möchten, und klicken Sie anschließend auf die Schaltfläche **Mit Remote-Desktop verbinden**.

   Das Fenster **Mit Remote-Desktop verbinden** wird geöffnet.

   Wenn Sie mehrere Geräte, ein Mobilgerät oder ein Gerät mit macOS auswählen, wird die Schaltfläche **Mit Remote-Desktop verbinden** deaktiviert.
3. Wählen Sie im Fenster **Mit Remote-Desktop verbinden** den Verbindungstyp **Windows Desktopfreigabe**.

   Wenn keine Lizenz für das Schwachstellen- und Patch-Management verfügbar ist, wird eine Fehlermeldung angezeigt.
4. Laden Sie das Tool "klsctunnel" herunter, indem Sie auf die Schaltfläche **Download** klicken, und führen Sie es anschließend aus.

   Wenn das Tool nicht zum Download verfügbar ist, wird eine Fehlermeldung angezeigt. Laden Sie das Tool in diesem Fall manuell herunter.
5. Wählen Sie in der Liste der auf dem Gerät verfügbaren aktiven Benutzersitzungen, die Sitzung aus, mit der Sie eine Verbindung herstellen möchten.

   Der Remote-Benutzer muss diese Verbindung zulassen. Wenn der Remote-Benutzer die Verbindung ablehnt oder die Verbindung nicht innerhalb der Timeout-Periode zulässt, wird eine Fehlermeldung angezeigt.
6. Generieren Sie ein Text-BLOB mit codierten Verbindungsparametern, indem Sie auf die Schaltfläche **BLOB generieren** klicken und den Text anschließend kopieren und in das entsprechende Feld des Tools "klsctunnel" einfügen.

   Ein Blob enthält die Einstellungen, die zum Herstellen einer Verbindung zwischen dem Administrationsserver und dem verwalteten Gerät erforderlich sind. Ein BLOB ist 3 Minuten lang gültig. Erzeugen Sie ein neues BLOB, wenn es abgelaufen ist.
7. Wenn Sie einen Proxyserver verwenden, geben Sie im Tool "klsctunnel" die Verbindungseinstellungen des Proxyservers an.

   Aktivieren Sie dafür das Kontrollkästchen **Proxyserver verwenden** und geben Sie anschließend die Verbindungseinstellungen an.
8. Klicken Sie auf die Schaltfläche **Port öffnen**.

   Das Tool "klsctunnel" zeigt die Adresse und den Port für die lokale Verbindung eines VNC-Clients für den Remote-Zugriff an.

Das Tool ermöglicht dem Remote-Benutzer, die Tunnelverbindung zu schließen. Bei einem Schließen der Tunnelverbindung wird die aktuelle Verbindung zum Remote-Desktop beendet.

Die Desktopfreigabe startet in einem neuen Fenster. Wenn Sie das Gerät steuern möchten, klicken Sie das Menü-Symbol () in der linken oberen Ecke des Fensters und wählen Sie anschließend **Interaktiver Modus** aus.

Mobile Geräte verwalten

Die Verwaltung von mobilen Geräten über Kaspersky Security Center erfolgt mithilfe der Funktion "Verwaltung mobiler Geräte". Sie müssen auf jedem mobilen Gerät einen Lizenzschlüssel hinzufügen, um die Sicherheitsanwendung zu aktivieren. Wenn Sie die mobilen Geräte Ihrer Unternehmensmitarbeiter verwalten möchten, aktivieren und konfigurieren Sie die Verwaltung mobiler Geräte.

Mit der Verwaltung mobiler Geräte können Sie die Android- und iOS-Geräte Ihrer Mitarbeiter verwalten. Der Schutz wird durch die App "Kaspersky Endpoint Security für Android" und das System zur Verwaltung von iOS-Geräten zur Verfügung gestellt. Beide sind auf den Geräten installiert. Diese mobilen Apps gewährleisten den Schutz mobiler Geräte vor Web-Bedrohungen, Viren und anderen bedrohlichen Programmen. Zur zentralen Verwaltung über Kaspersky Security Center Web Console müssen Sie auf dem Gerät, auf dem die Kaspersky Security Center Web Console installiert ist, die folgenden Verwaltungs-Plug-in installieren:

- Kaspersky Mobile Devices Protection and Management

  Das Plug-in "Kaspersky Mobile Devices Protection and Management" ermöglicht die Verwaltung von Android- und iOS-Geräten über Kaspersky Security Center Web Console.

- Einstellungen des iOS MDM-Servers

  Das Plug-in für die Einstellungen des iOS MDM-Servers erlaubt Ihnen die Konfiguration des iOS MDM-Servers. Dieser wird verwendet, um iOS-Geräte mit dem Administrationsserver zu verbinden und iOS-Geräte zu verwalten.

Weitere Informationen zur Bereitstellung des Schutzes und zur Verwaltung mobiler Geräte finden Sie in der Hilfe zu Kaspersky Security für mobile Endgeräte und in der Hilfe zu Kaspersky Secure Mobility Management.

Verwendung von Firebase Cloud Messaging

Um die zeitnahe Übermittlung von Befehlen an Android-Geräte zu ermöglichen, verwendet Kaspersky Security Center Linux Push-Benachrichtigungen. Push-Benachrichtigungen zwischen Android-Geräten und dem Administrationsserver werden mittels Firebase Cloud Messaging (im Folgenden mit "FCM" abgekürzt) ausgetauscht. In der Kaspersky Security Center Web Console können Sie die Einstellungen für Firebase Cloud Messaging festlegen, um Android-Geräte mit dem Dienst zu verbinden.

Um die Einstellungen für Firebase Cloud Messaging abzurufen, müssen Sie über ein Google-Benutzerkonto verfügen.

So aktivieren die Verwendung von FCM:

1. Wählen Sie im Hauptfenster der Kaspersky Security Center Web Console den Punkt **Asset-Verwaltung** → **Mobile** → **Devices** aus.

2. Öffnen Sie das 3-Punkte-Menü (⋮) und wählen Sie **Forced Android device synchronization** aus.

3. Geben Sie im Feld **Firebase project number** die FCM-Sender-ID an.

4. Wählen Sie im Feld **Private key** die Datei mit dem privaten Schlüssel aus.

   Bei der nächsten Synchronisierung mit dem Administrationsserver werden die Android-Geräte mit Firebase Cloud Messaging verbunden.

Wenn Sie zu einem anderen Firebase-Projekt wechseln, müssen Sie 10 Minuten warten, bis FCM fortgesetzt wird.

Der Dienst FCM arbeitet in den folgenden Adressbereichen:

- Seitens der Android-Geräte ist der Zugriff auf die Ports 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) und 5230 (HTTPS) der folgenden Adressen erforderlich:
  - google.com
  - fcm.googleapis.com
  - oauth2.googleapis.com
  - android.apis.google.com
  - Alle IP-Adressen aus der Liste "Google ASN 15169"
- Seitens des Administrationsservers ist der Zugriff auf den Port 443 (HTTPS) der folgenden Adressen erforderlich:
  - fcm.googleapis.com
  - Oder auf allen IP aus der Liste "Google ASN 15169"

Falls in der Kaspersky Security Center Web Console die Proxyserver-Einstellungen in den Eigenschaften des Administrationsservers festgelegt wurden, werden sie für die Interaktion mit FCM verwendet.

Konfiguration von FCM: Sender-ID und Datei mit dem privaten Schlüssel abrufen

So konfigurieren Sie FCM:

1. Registrieren Sie sich auf dem Google-Portal.

2. Gehen Sie zur Firebase-Konsole.

3. Führen Sie eine der folgenden Aktionen aus:

   - Erstellen Sie ein neues Projekt, indem Sie auf **Projekt erstellen** klicken und den Anweisungen auf dem Bildschirm folgen.
   - Öffnen Sie ein vorhandenes Projekt.

4. Klicken Sie auf das Zahnrad-Symbol und wählen Sie **Projekteinstellungen** aus.

   Das Fenster **Projekteinstellungen** wird geöffnet.

5. Wählen Sie die Registerkarte **Cloud Messaging** aus.

6. Rufen Sie die relevante Sender-ID aus dem Feld **Sender ID** im Abschnitt **Firebase Cloud Messaging API (V1)** ab.

7. Wählen Sie die Registerkarte **Dienstkonten** aus und klicken Sie auf **Neuen privaten Schlüssel generieren**.

8. Klicken Sie im neuen Fenster auf **Schlüssel generieren**, um eine Datei mit einem privaten Schlüssel zu generieren und herunterzuladen.

Firebase Cloud Messaging ist jetzt konfiguriert.

Integration mit Public Key Infrastructure

Sie können die Ausstellung von Zertifikaten durch die Microsoft-Zertifizierungsstelle (CA) mittels einer Public-Key-Infrastruktur (PKI) integrieren. Die PKI-Integration soll die Ausstellung von Zertifikaten für Domänenbenutzer durch den Administrationsserver vereinfachen. Nach der Integration werden Zertifikate automatisch ausgestellt.

Ausführliche Informationen über die Konfiguration der PKI-Integration zur Zertifikatsausstellung finden Sie in der Hilfe zu Kaspersky Secure Mobility Management.

Sie können die PKI-Integration mit den angegebenen Einstellungen durchführen und die PKI als Quelle für Zertifikate für bestimmte Arten von Zertifikaten zuweisen. In den Einstellungen der PKI-Integration können Sie die individuelle Standardvorlage für alle Arten von Zertifikaten festlegen.

Besonderheiten bei der Verwendung der PKI-Integration zur Zertifikatsausstellung:

- Die PKI-Integration ist standardmäßig deaktiviert. Ausführliche Informationen zur Aktivierung der PKI und zur Konfiguration der Einstellungen finden Sie in der Hilfe zu Kaspersky Secure Mobility Management.

- Die Zertifikatsausstellung erfolgt mithilfe des Windows-Administrationsagenten, der die Integration zwischen dem Administrationsserver und der Microsoft-Zertifizierungsstelle ermöglicht. Da der Administrationsagent auf mehreren Geräten installiert sein kann, können Sie in den **Issuance rules** das Gerät angeben, das eine Verbindung mit der Microsoft-Zertifizierungsstelle herstellt. Auf dem Gerät muss ein Zertifikat für einen Enrollment Agent (EA) in dem Zertifikatsspeicher des Benutzerkontos installiert sein, unter dem die PKI-Integration ausgeführt wird. Das Zertifikat wird vom Administrator der Domänen-Zertifizierungsstelle ausgestellt.

- Das Benutzerkonto, unter dem die PKI-Integration ausgeführt wird, muss ein Domänenbenutzer sein und über die Berechtigung *Als Dienst anmelden* verfügen.

- Kaspersky Security Center Linux kann jeweils nur mit einer PKI-Integration (Microsoft CA) ausgeführt werden.

Administrationsgruppen verwalten

Der Abschnitt enthält Informationen über die Arbeit mit den Administrationsgruppen.

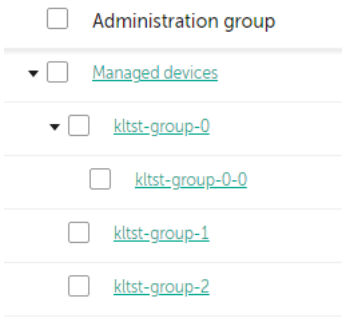
Sie können mit den Administrationsgruppen folgende Aktionen ausführen:

- eine beliebige Anzahl von untergeordneten Gruppen aller Hierarchieebenen zu einer Administrationsgruppe hinzufügen
- Geräte zu Administrationsgruppen hinzufügen
- Hierarchie der Administrationsgruppen durch Verschieben einzelner Geräte und ganzer Gruppen in andere Gruppen ändern
- Untergruppen und Geräte aus Administrationsgruppen löschen
- Dem Verzeichnis der Administrationsgruppen sekundäre und virtuelle Administrationsserver hinzufügen
- Geräte aus Administrationsgruppen eines Administrationsservers in die Gruppen eines anderen Servers verschieben
- Festlegen, welche Kaspersky-Anwendungen automatisch auf den Geräten installiert werden sollen, die in eine Gruppe aufgenommen werden

Sie können diese Aktionen nur dann durchführen, wenn Sie die Berechtigung **Ändern** im Bereich **Verwaltung von Administrationsgruppen** für die Administrationsgruppe (oder für den Administrationsserver, zu dem diese Gruppen gehören) haben, die Sie ändern wollen.

Administrationsgruppen anlegen

Unmittelbar nach der Installation von Kaspersky Security Center enthält die Hierarchie der Administrationsgruppen nur eine einzige Administrationsgruppe mit dem Namen: **Verwaltete Geräte**. Wenn Sie eine Hierarchie der Administrationsgruppen erstellen, können Sie Geräte, virtuelle Maschinen und untergeordnete Gruppen zur Gruppe **Verwaltete Geräte** hinzufügen (siehe folgende Abbildung).

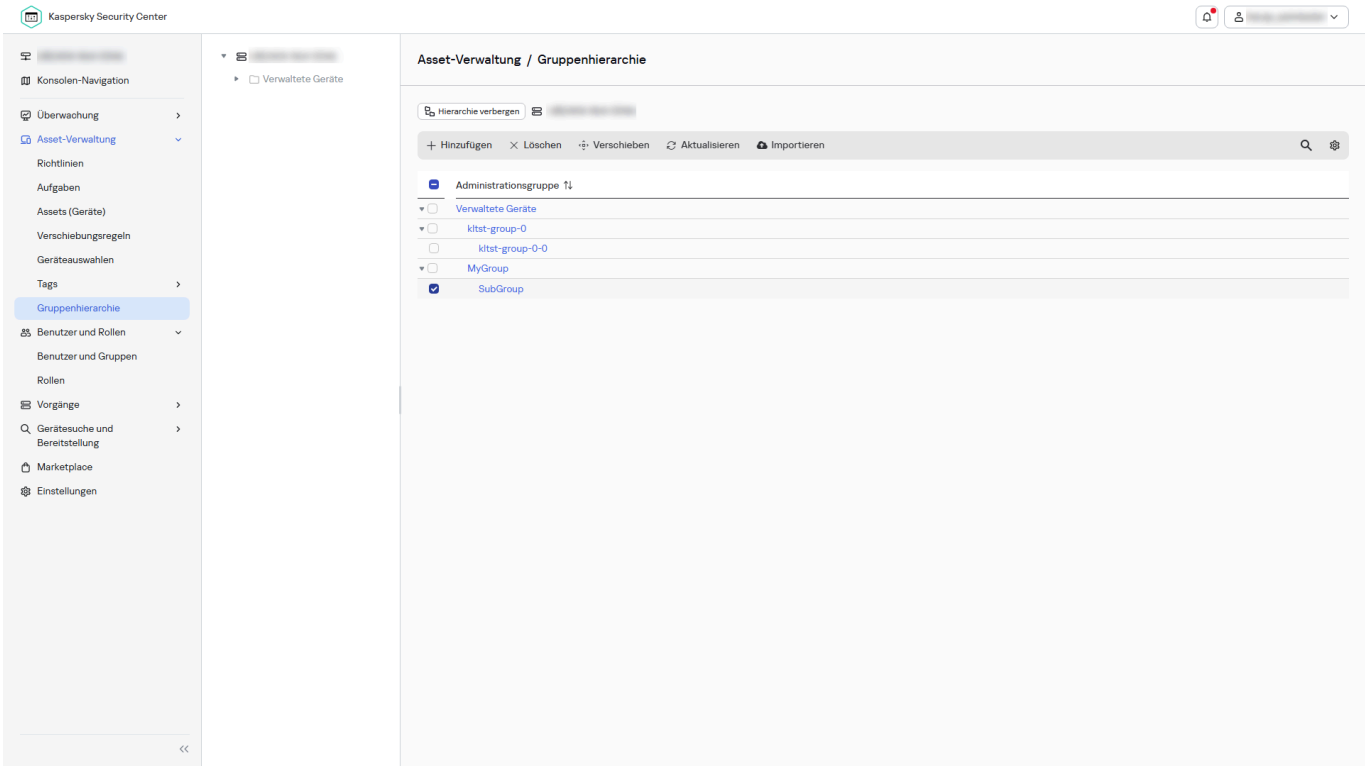


Hierarchie der Administrationsgruppen erstellen

Um eine Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

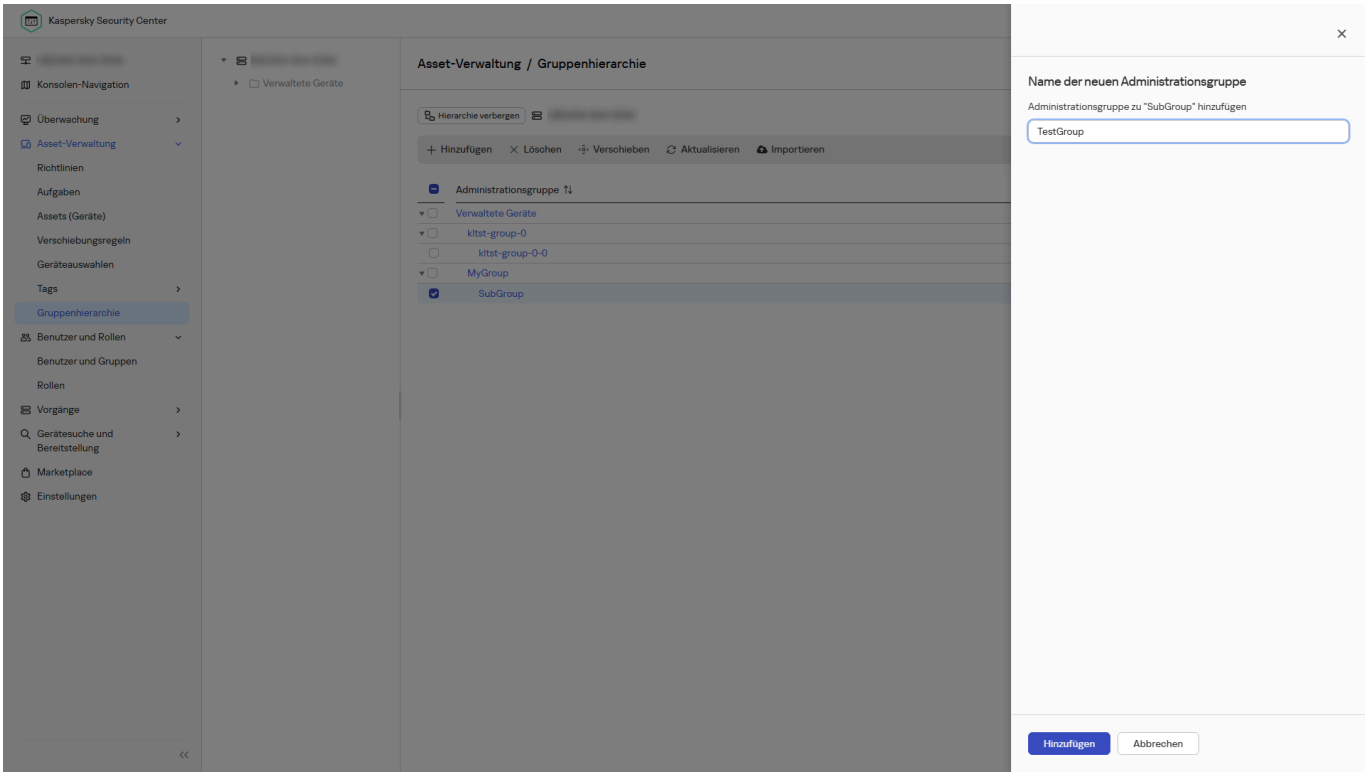
1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Gruppenhierarchie**.

2. Wählen Sie in der Hierarchie der Administrationsgruppen die Administrationsgruppe aus, welche die neue Administrationsgruppe enthalten soll.



3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

4. Geben Sie im folgenden Fenster **Name der neuen Administrationsgruppe** den Namen der Gruppe ein, und klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.



In der Hierarchie der Administrationsgruppen erscheint eine neue Administrationsgruppe mit dem angegebenen Namen.

Um die Struktur der Administrationsgruppe zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Gruppenhierarchie**.
2. Klicken Sie auf die Schaltfläche **Importieren**.

Daraufhin wird der Assistent für das Erstellen einer Administrationsgruppenstruktur gestartet. Folgen Sie den Anweisungen des Assistenten.

Programme automatisch auf Geräten einer Administrationsgruppe installieren

Sie können angeben, welche Installationspakete für die automatische Remote-Installation von Kaspersky-Anwendungen auf Client-Geräten in einer Administrationsgruppe verwendet werden sollen.

Um die automatische Installation von Anwendungen auf den Geräten in einer Administrationsgruppe zu konfigurieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Gruppenhierarchie**.
2. Wechseln Sie auf eine der folgenden Arten zu den Eigenschaften der erforderlichen Administrationsgruppe:
   - Klicken Sie auf den Namen der Administrationsgruppe.
   - Klicken Sie im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**. Bewegen Sie im neuen Navigationsbereich den Mauszeiger über den Namen der gewünschten Gruppe und klicken Sie anschließend auf das Einstellungssymbol (⚙).

   Das Eigenschaftenfenster der übergeordneten Administrationsgruppe wird geöffnet.
3. Wechseln Sie im Eigenschaftsfenster auf die Registerkarte **Automatische Installation**.
4. Wählen Sie die Installationspakete für die Anwendungen aus, die auf den Geräten installiert werden sollen, und bestätigen Sie anschließend auf die Schaltfläche **Speichern**.

   Wenn Sie für eine Anwendung mehrere Installationspakete auswählen, die sich lediglich in ihren Versionen unterscheiden, wird das Installationspaket der aktuellsten Version gespeichert.

Nachdem Sie die Installationspakete ausgewählt haben, wird für jede Anwendung eine Gruppenaufgabe zur Installation der Anwendungen auf den Geräten der Administrationsgruppe erstellt. Diese Aufgaben werden auf den Client-Geräten gestartet, direkt nachdem diese zu der Administrationsgruppe hinzugefügt wurden.

Administrationsgruppen verschieben

Sie können untergeordnete Administrationsgruppen innerhalb der Hierarchie der Gruppen verschieben.

Die Administrationsgruppe wird zusammen mit allen Untergruppen, sekundären Administrationsservern, Geräten sowie Gruppenrichtlinien und -aufgaben verschoben. Das System wendet sämtliche Einstellungen auf die Gruppe an, die ihrer neuen Position in der Hierarchie der Administrationsgruppen entsprechen.

Der Gruppenname muss innerhalb einer Hierarchieebene einmalig sein. Wenn im Ordner, in den Sie die Administrationsgruppe verschieben, eine Gruppe mit dem gleichen Namen bereits vorhanden ist, ändern Sie den Namen der Gruppe vor dem Verschieben. Wenn Sie den Namen der zu verschiebenden Gruppe zuvor nicht geändert haben, wird dem Namen der Gruppe beim Verschieben die Endung **_<laufende Nummer>** (z.B. **(1)**, **(2)**) hinzugefügt.

Die Gruppe **Verwaltete Geräte** kann weder umbenannt noch verschoben werden.

So verschieben Sie eine Administrationsgruppe innerhalb der Hierarchie der Administrationsgruppen in eine andere Ebene:

1. Rufen Sie im Hauptmenü den Abschnitt **Asset-Verwaltung** → **Gruppenhierarchie** auf und aktivieren Sie anschließend das Kontrollkästchen neben der Administrationsgruppe, die Sie verschieben möchten.
2. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Verschieben**.
3. Wählen Sie im neuen Fenster aus, wohin Sie die Administrationsgruppe verschieben möchten, und klicken Sie anschließend auf die Schaltfläche **Verschieben**.

   Das Fenster schließt sich und die Administrationsgruppe wird in eine andere Ebene der Gruppenhierarchie verschoben.

Deleting administration groups

Wenn Sie eine Administrationsgruppe löschen, die sekundäre Administrationsserver, verschachtelte Gruppen, Client-Geräte, Gruppenaufgaben oder für diese Gruppe erstellte Richtlinien enthält, werden diese ebenfalls alle gelöscht.

Bevor eine Administrationsgruppe gelöscht wird, ist es erforderlich, sekundäre Administrationsserver, Gruppen und Client-Geräte daraus zu löschen.

So löschen Sie eine Administrationsgruppe:

1. Rufen Sie im Hauptmenü den Abschnitt **Asset-Verwaltung** → **Gruppenhierarchie** auf und aktivieren Sie anschließend das Kontrollkästchen neben der Administrationsgruppe, die Sie löschen wollen.
2. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Löschen**.

   Die Benutzergruppe wird gelöscht.

Kaspersky-Anwendungen bereitstellen

Dieser Abschnitt beschreibt die Bereitstellung von Kaspersky-Anwendungen auf Client-Geräten in Ihrem Unternehmen mithilfe von Kaspersky Security Center Web Console.

Szenario: Kaspersky-Programme bereitstellen

Dieses Szenario erklärt, wie Kaspersky-Anwendungen über Kaspersky Security Center Web Console verteilt werden. Sie können den Schnellstartassistenten und den Assistenten für die Bereitstellung des Schutzes verwenden oder alle erforderlichen Schritte manuell ausführen.

Die folgenden Anwendungen können über die Kaspersky Security Center Web Console verteilt werden:

- Kaspersky Endpoint Security für Linux
- Kaspersky Endpoint Security für Windows

Schritte

Die Bereitstellung von Kaspersky-Anwendungen erfolgt schrittweise:

1. **Download des Verwaltungs-Web-Plug-ins für die Anwendung**

   Diese Etappe ist Teil des Schnellstartassistenten. Wenn Sie den Assistenten nicht ausführen möchten, können Sie die Plug-ins manuell herunterladen.

2. **Installationspakete herunterladen und erstellen**

   Diese Etappe ist Teil des Schnellstartassistenten.

   Mithilfe des Schnellstartassistenten können Sie das Installationspaket mit dem Verwaltungs-Web-Plug-in herunterladen. Wenn Sie diese Option beim Ausführen des Assistenten nicht ausgewählt haben oder wenn Sie den Assistenten nicht ausgeführt haben, müssen Sie das Paket manuell herunterladen.

   Wenn die Installation von Kaspersky-Anwendungen mithilfe von Kaspersky Security Center Linux auf bestimmten Geräten nicht möglich ist (z. B. auf Geräten von Remote-Mitarbeitern), können Sie autonome Installationspakete für Anwendungen erstellen. Wenn Sie für die Installation von Kaspersky-Anwendungen autonome Pakete verwenden, müssen Sie weder eine Aufgabe zur Remote-Installation erstellen und ausführen noch Aufgaben für Kaspersky Endpoint Security für Windows erstellen und konfigurieren.

   Alternativ können Sie die Programmpakete für den Administrationsagenten und die Sicherheitsanwendungen von der Kaspersky-Website herunterladen. Wenn die Remote-Installation der Anwendungen aus irgendeinem Grund nicht möglich ist, können Sie die heruntergeladenen Programmpakete verwenden, um die Anwendungen lokal zu installieren.

3. **Erstellen, Konfigurieren und Ausführen der Remote-Installationsaufgabe**

   Dieser Schritt ist Teil des Assistenten für die Bereitstellung des Schutzes. Wenn Sie den Assistenten für die Bereitstellung des Schutzes nicht ausführen möchten, müssen Sie diese Aufgabe manuell erstellen und konfigurieren.

   Manuell können Sie mehrere Remote-Installationsaufgaben für verschiedene Administrationsgruppen oder unterschiedliche Geräteauswahlen erstellen. Sie können in diesen Aufgaben verschiedene Versionen einer Anwendung bereitstellen.

Stellen Sie sicher, dass alle Geräte in Ihrem Netzwerk erkannt wurden. Starten Sie dann die Aufgabe (Aufgaben) zur Remote-Installation.

Wenn Sie den Administrationsagenten auf Geräten mit dem Betriebssystem SUSE Linux Enterprise Server 15 installieren möchten, sollten Sie zunächst das Paket insserv-compat installieren, um den Administrationsagenten konfigurieren.

Wenn Sie den Administrationsagenten auf Geräten mit den Betriebssystemen RED OS 7.3.4 und höher bzw. MSVSPHERE 9.2 und höher installieren möchten, installieren Sie das Paket "libxcrypt-compat", damit der Administrationsagent ordnungsgemäß funktioniert.

4. **Erstellen und Konfigurieren von Aufgaben**

   Die *Update*-Aufgabe von Kaspersky Endpoint Security muss konfiguriert werden.

   Dieser Schritt ist Teil des Schnellstartassistenten: Die Aufgabe wird automatisch mit den Standardeinstellungen erstellt und konfiguriert. Wenn Sie den Assistenten nicht ausgeführt haben, müssen Sie diese Aufgabe manuell erstellen und auch manuell konfigurieren. Wenn Sie den Schnellstartassistenten verwenden, stellen Sie sicher, dass der Zeitplan für die Aufgabe Ihren Anforderungen entspricht (Standardmäßig ist der geplante Start für die Aufgabe auf **Manuell** eingestellt; möglicherweise möchten Sie eine andere Option auswählen).

5. **Richtlinien anlegen**

   Erstellen Sie die Richtlinie für Kaspersky Endpoint Security entweder manuell oder über den Schnellstartassistenten. Sie können die Standardeinstellungen der Richtlinie verwenden. Sie können jedoch die Standardeinstellungen der Richtlinie jederzeit gemäß Ihren Anforderungen ändern.

6. **Untersuchung der Ergebnisse**

   Stellen Sie sicher, dass die Bereitstellung erfolgreich beendet wurde, das heißt: Jede Anwendung besitzt Richtlinien und Aufgaben und diese Anwendungen sind auf den verwalteten Geräten installiert.

Ergebnisse

Der Abschluss des Szenarios bringt folgende Ergebnisse mit sich:

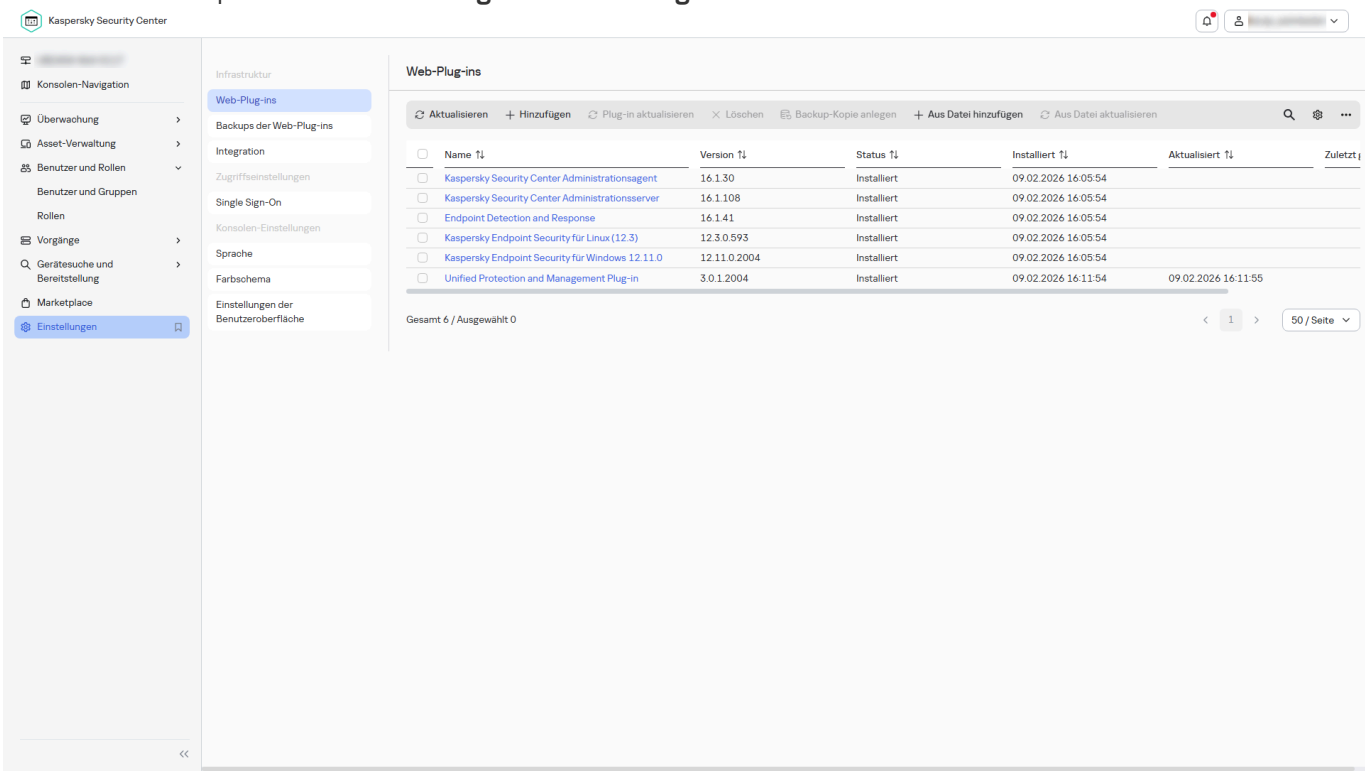
- Es werden alle erforderlichen Richtlinien und Aufgaben für die ausgewählten Anwendungen erstellt.
- Die Zeitpläne der Aufgaben werden gemäß Ihren Anforderungen angepasst.
- Die ausgewählten Anwendungen wurden auf den ausgewählten Client-Geräten verteilt oder werden nach Zeitplan verteilt.

Verwaltungs-Plug-ins für Kaspersky-Anwendungen hinzufügen

Um eine Kaspersky-Anwendung wie beispielsweise Kaspersky Endpoint Security für Linux oder Kaspersky Endpoint Security für Windows zu bereitzustellen, müssen Sie das entsprechende Verwaltungs-Web-Plug-in herunterladen und hinzufügen.

So laden Sie ein Verwaltungs-Web-Plug-in für eine Kaspersky-Anwendung herunter:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Web-Plug-ins**.



Die Liste der installierten Web-Plug-ins

2. Klicken Sie im folgenden Fenster auf **Hinzufügen**.

   Eine Liste der verfügbaren Plug-ins wird angezeigt.

3. Wählen Sie in der Liste der verfügbaren Plug-ins das Plug-in aus, das Sie herunterladen möchten (z. B. Kaspersky Endpoint Security für Linux), indem Sie auf seinen Namen klicken.

   Die Seite mit der Beschreibung des Plug-ins wird angezeigt.

4. Klicken Sie auf der Seite mit der Beschreibung des Plug-ins auf **Plug-in installieren**.

5. Klicken Sie nach Abschluss der Installation auf **OK**.

Das Verwaltungs-Web-Plug-in wird mit der Standardkonfiguration heruntergeladen und in der Liste mit Verwaltungs-Web-Plug-ins angezeigt.

Sie können Plug-ins hinzuzufügen und heruntergeladene Plug-ins aus einer Datei aktualisieren. Sie können die Web-Plug-ins zur Verwaltung von der Kaspersky-Website herunterladen.

So können Sie ein Verwaltungs-Web-Plug-in herunterladen oder aus einer Datei aktualisieren:

1. Wechseln Sie im Hauptmenü zu **Einstellungen** → **Web-Plug-ins**.

2. Geben Sie die Datei des Plug-ins sowie die Dateisignatur an:

   - Klicken Sie auf **Aus Datei hinzufügen**, um ein Plug-in aus einer Datei herunterzuladen.
   - Klicken Sie auf **Aus Datei aktualisieren**, um das Update für ein Plug-in aus einer Datei herunterzuladen.

3. Geben Sie die Datei und die Dateisignatur an.

4. Laden Sie die angegebenen Dateien herunter.

   Das Verwaltungs-Web-Plug-in wird aus der Datei heruntergeladen und in der Liste mit Verwaltungs-Web-Plug-ins angezeigt.

Installationspakete

Ein *Installationspaket* ist ein Paket mit Dateien, das zur Remote-Installation einer Kaspersky-Anwendung erstellt wird. Das Installationspaket enthält eine Reihe von Einstellungen, die für die Installation und Inbetriebnahme der Anwendung nach der Installation benötigt werden. Die Einstellungen entsprechen der Standardkonfiguration der Anwendung. Das Installationspaket wird mithilfe von Dateien mit kpd- und kud-Erweiterungen erstellt, die im Lieferumfang der Anwendung enthalten sind.

Die Installationspakete werden auf folgende Arten erstellt:

- Automatisch aus den angegebenen Programmpaketen auf der Grundlage *Beschreibungen* in ihren Bestand (Dateien mit der Erweiterung kud, die Regeln für Installation und Analyse des Ergebnisses und andere Informationen enthalten)

- Aus einer zip-, cab-, tar- oder tar.gz-Archivdatei für Standardanwendungen oder unterstützte Anwendungen.

Die erstellten Installationspakete bestehen aus einer Hierarchie von Ordnern mit Unterordnern und Dateien. Neben den originalen Programmpaketen umfasst das Installationspaket die bearbeiteten Einstellungen (einschließlich der Einstellungen des Installers und der Regel zur Verarbeitung von Situationen wie ein erforderlicher für den Abschluss der Installation Neustart des Betriebssystems), sowie kleine Hilfsmodule.

Die Werte der Installationseinstellungen, die spezifisch für die konkrete unterstützte App sind, können in der Benutzerschnittstelle der Kaspersky Security Center Web Console beim Erstellen des Installationspakets festgelegt werden. Im Fall einer Remote-Installation der Apps mithilfe von Kaspersky Security Center Linux werden die Installationspakete so an die Geräte so geliefert, dass beim Start des Installers der App alle vom Administrator festgelegten Einstellungen verfügbar sind. Bei Verwendung von Drittanbieter-Tools zur Installation von Kaspersky-Anwendungen müssen Sie nur sicherstellen, dass auf dem Gerät das komplette Installationspaket verfügbar ist, also das Programmpaket und dessen Einstellungen. Die Installationspakete werden erstellt und von Kaspersky Security Center Linux im entsprechenden Unterordner des freigegebenen Ordners aufbewahrt.

Geben Sie in den Einstellungen der Installationspakete keine Daten von privilegierten Benutzerkonten an.

Die Bereitstellung mithilfe des Mechanismus der Gruppenrichtlinien von Microsoft Windows wird nicht unterstützt.

Sofort nach der Installation von Kaspersky Security Center Linux werden automatisch mehrere Installationspakete erstellt, die bereit zur Installation sind, darunter die Pakete des Administrationsagenten und der Sicherheitsanwendungen für die Plattform Microsoft Windows.

Obwohl es möglich ist, den Lizenzschlüssel für das Programm in den Eigenschaften des Installationspakets anzugeben, sollte diese Methode der Lizenzverteilung nicht verwendet werden, da es in diesem Fall einfach ist, Lesezugriff auf Installationspakete zu erlangen. Es wird empfohlen, automatisch verteilte Lizenzschlüssel oder Aufgaben zur Installation von Lizenzschlüsseln zu verwenden.

Installationspakete für Kaspersky-Anwendungen herunterladen und erstellen

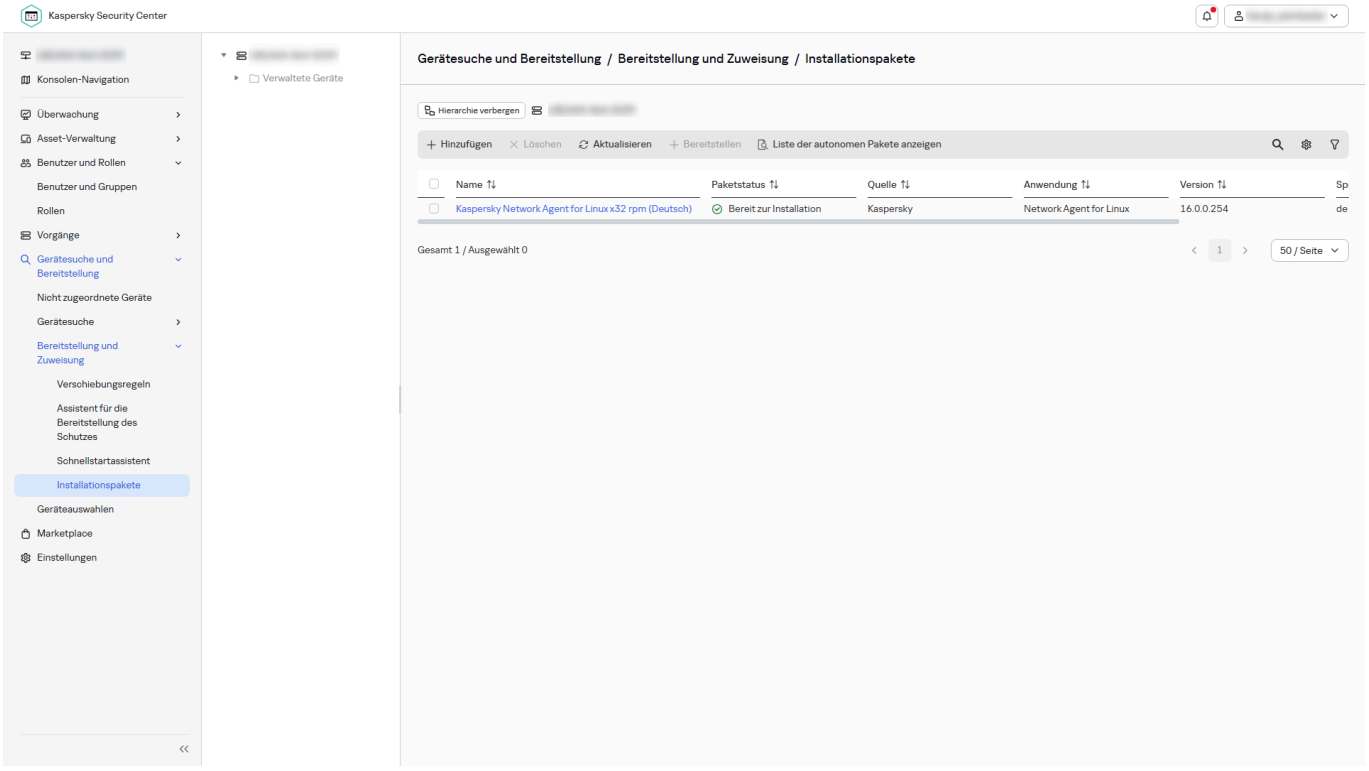
Wenn Ihr Administrationsserver über einen Internetzugang verfügt, können Sie die Installationspakete für Kaspersky-Anwendungen über die Kaspersky-Webserver erstellen.

Um ein Installationspaket für eine Kaspersky-Anwendung herunterzuladen und zu erstellen:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung** → **Installationspakete**.

   Benachrichtigungen über neue Pakete für Kaspersky-Anwendungen können Sie auch in der Liste der Benachrichtigungen auf dem Bildschirm anzeigen. Wenn es Benachrichtigungen über ein neues Paket gibt, können Sie auf den Link neben der Benachrichtigung klicken und zur Liste der verfügbaren Installationspakete wechseln.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

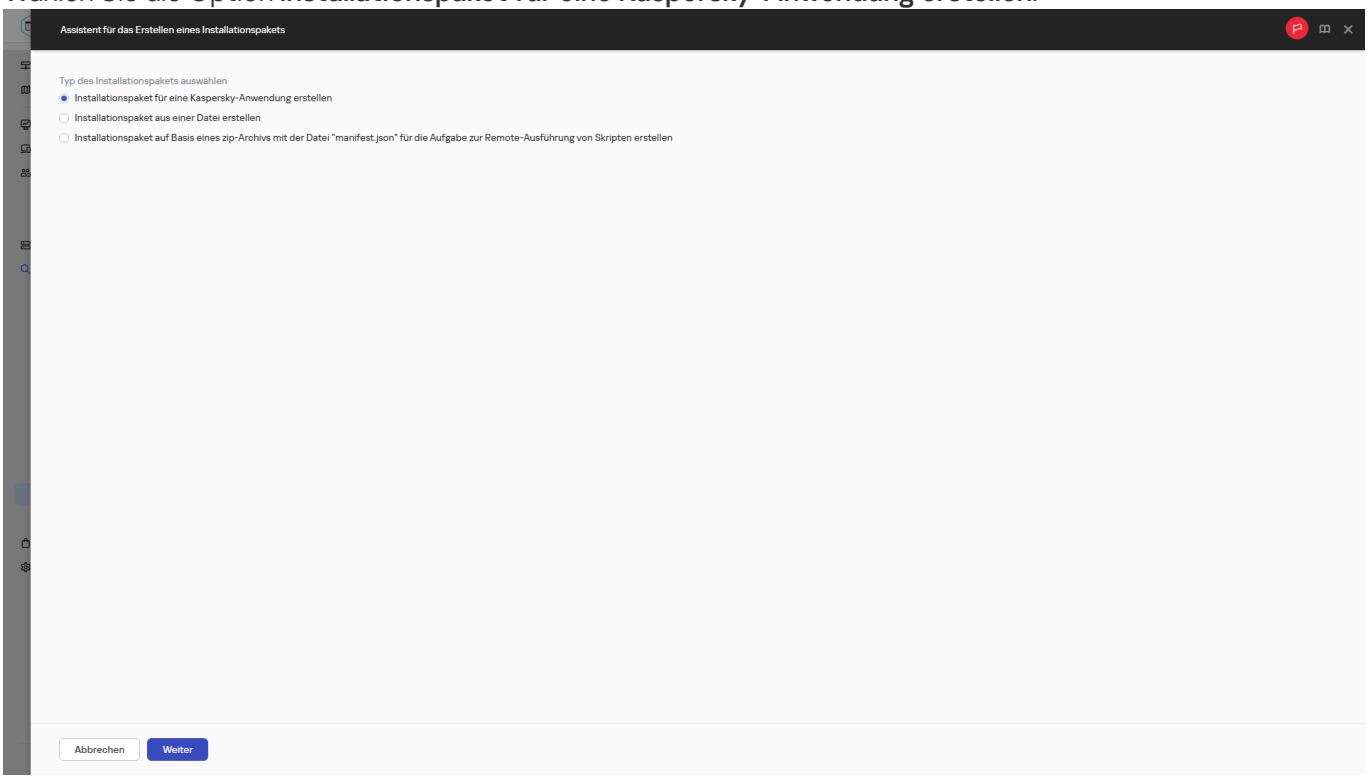


Die Liste der Installationspakete

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

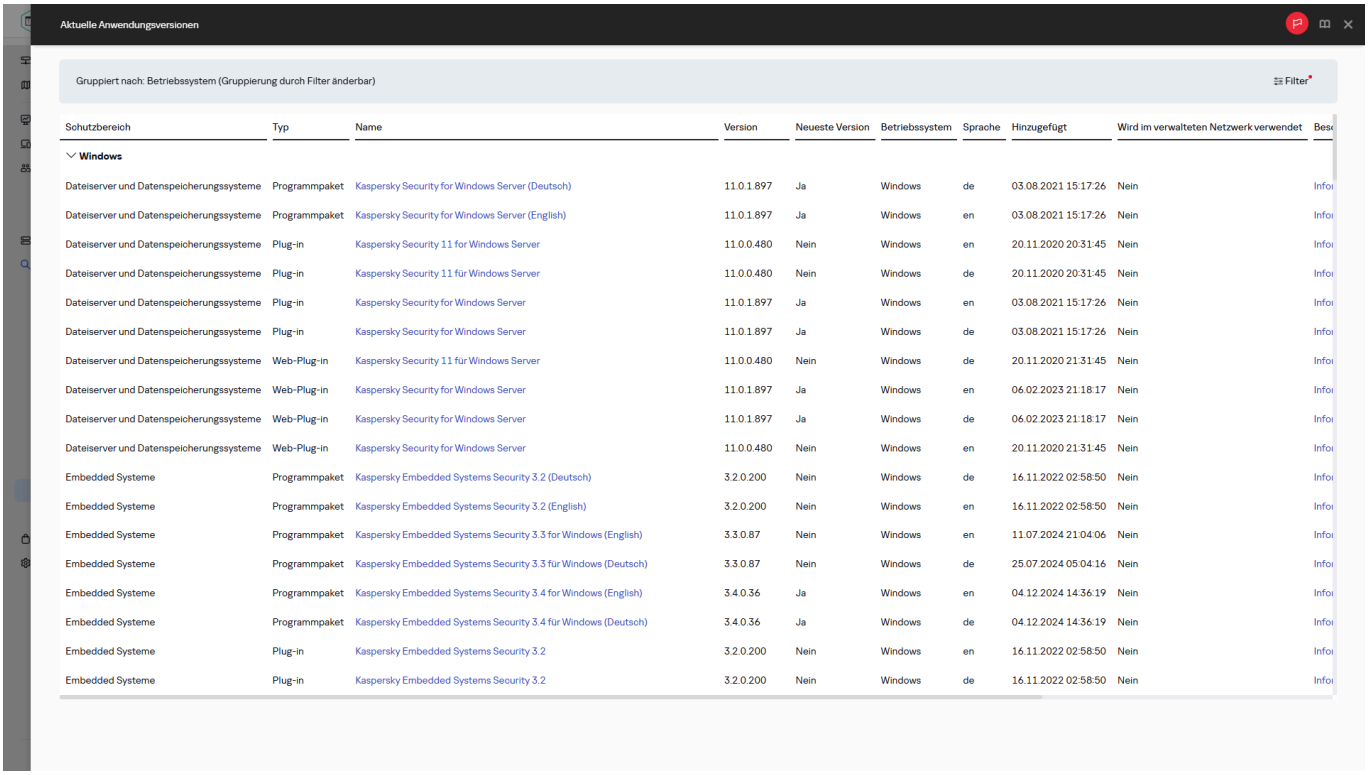
   Der Assistent für das Erstellen eines Installationspakets wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie die Option **Installationspaket für eine Kaspersky-Anwendung erstellen**.



Typ des Installationspakets auswählen

Eine Liste der Installationspakete, die auf den Kaspersky-Webservern verfügbar sind, wird angezeigt. Die Liste enthält nur Installationspakete von den Anwendungen, die zu der aktuell genutzten Version von Kaspersky Security Center Linux kompatibel sind. Standardmäßig werden in der Liste nur Anwendungen in Englisch sowie in der Sprache angezeigt, die der Schnittstelle entspricht. Um weitere Sprachen anzuzeigen, klicken Sie auf **„Filter“** und konfigurieren Sie die Filtereinstellungen.

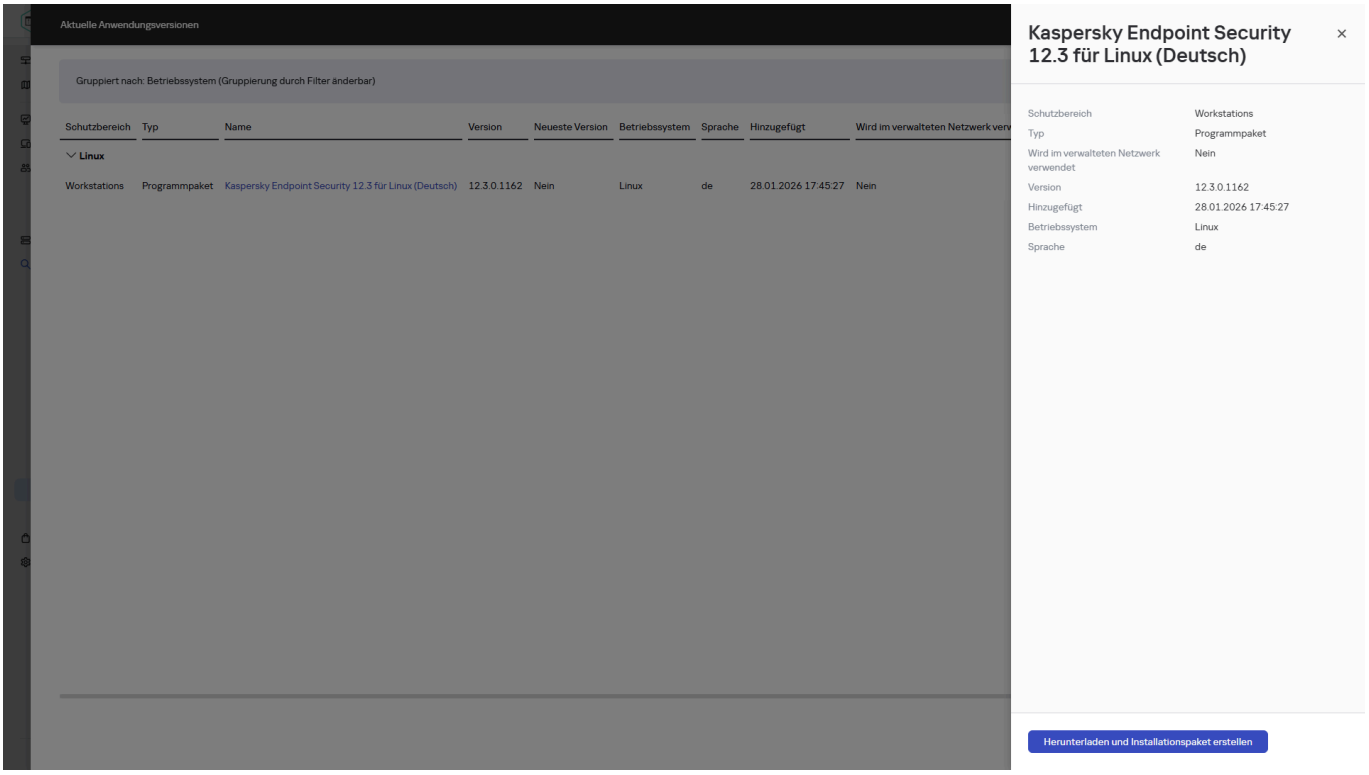


Die Liste der verfügbaren Installationspakete

4. Klicken Sie auf den Namen eines Installationspakets, z. B. Kaspersky Endpoint Security für Linux.

   Ein Fenster mit Informationen über das Installationspaket wird geöffnet.

Sie können ein Installationspaket mit kryptografischen Tools, die eine starke Verschlüsselung implementieren, herunterladen und verwenden, wenn es den geltenden Gesetzen und Vorschriften entspricht. Um ein Installationspaket von Kaspersky Endpoint Security für Windows herunterzuladen, dass den Bedürfnissen Ihrer Organisation entspricht, konsultieren Sie die Gesetzgebung in dem Land, in dem sich die Client-Geräte Ihrer Organisation befinden.



Herunterladen des Installationspakets

5. Lesen Sie die Informationen und klicken Sie auf **Herunterladen und Installationspaket erstellen**.

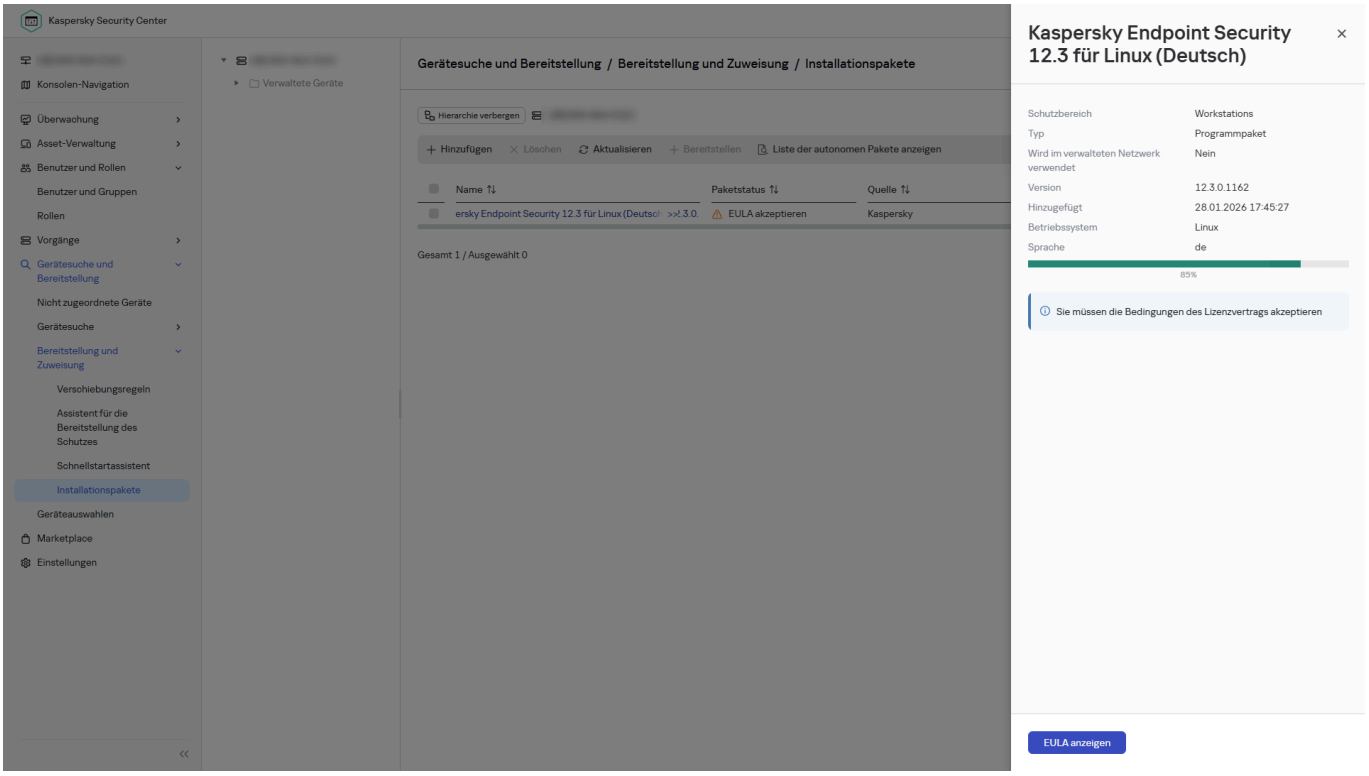
   Wenn ein Programmpaket nicht in ein Installationspaket konvertiert werden kann, wird die Schaltfläche **Programmpaket herunterladen** anstelle der Schaltfläche **Herunterladen und Installationspaket erstellen** angezeigt.

Bei einigen Kaspersky-Anwendungen wird vor oder während des Downloads die Schaltfläche **EULA anzeigen** angezeigt. Wenn die Schaltfläche angezeigt wird, gehen Sie wie folgt vor:

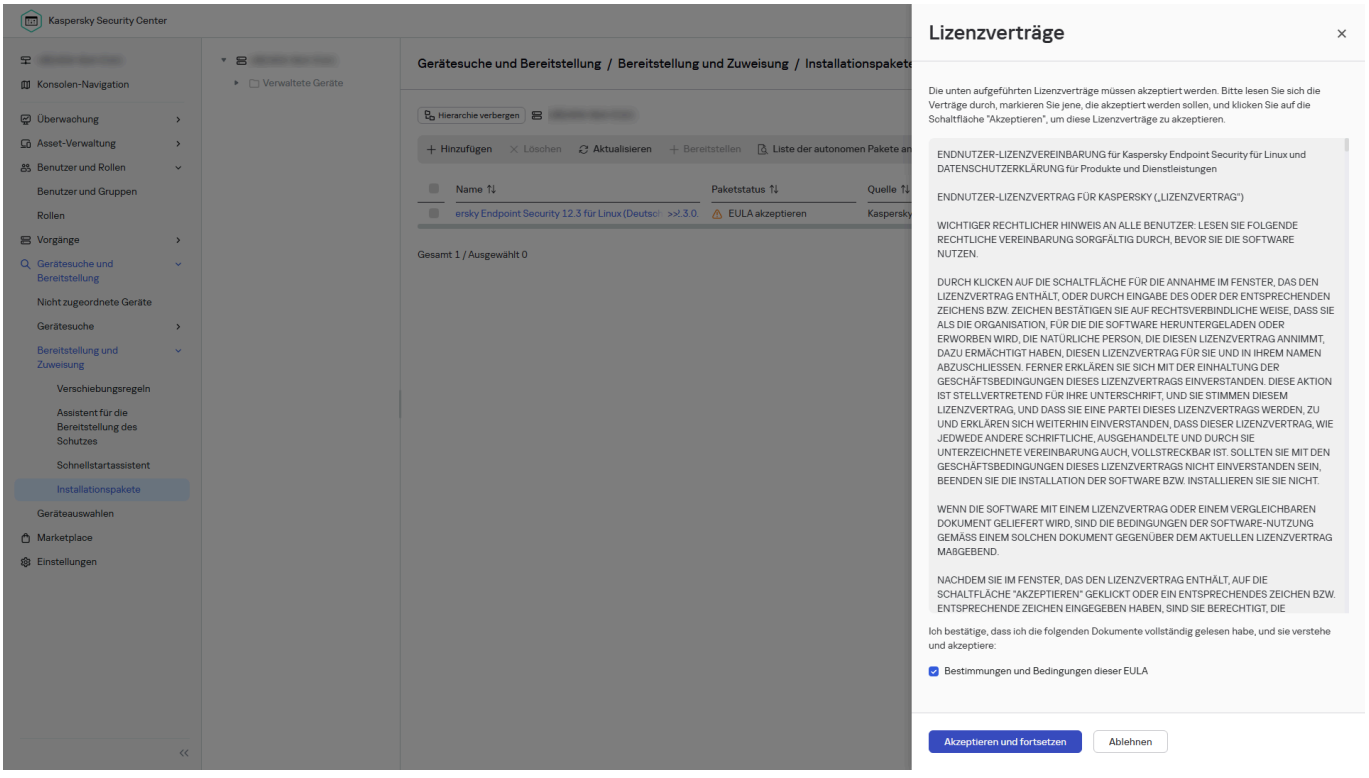
a. Klicken Sie auf **EULA anzeigen**, um den Endbenutzer-Lizenzvertrag (EULA) zu lesen.

b. Lesen Sie die EULA, die auf dem Bildschirm angezeigt wird, und klicken Sie auf **Akzeptieren**.

Der Download wird fortgesetzt, nachdem Sie die EULA akzeptiert haben. Wenn Sie auf **Ablehnen** klicken, wird der Download beendet.



Herunterladen des Installationspakets



Akzeptieren der EULA

Sie können das Fenster des Assistenten schließen. In diesem Fall wird der Download im Hintergrund fortgesetzt. In der Spalte **Paketstatus** können Sie den Download-Status des Installationspakets verfolgen, sowie Filter anwenden und nach Status sortieren.

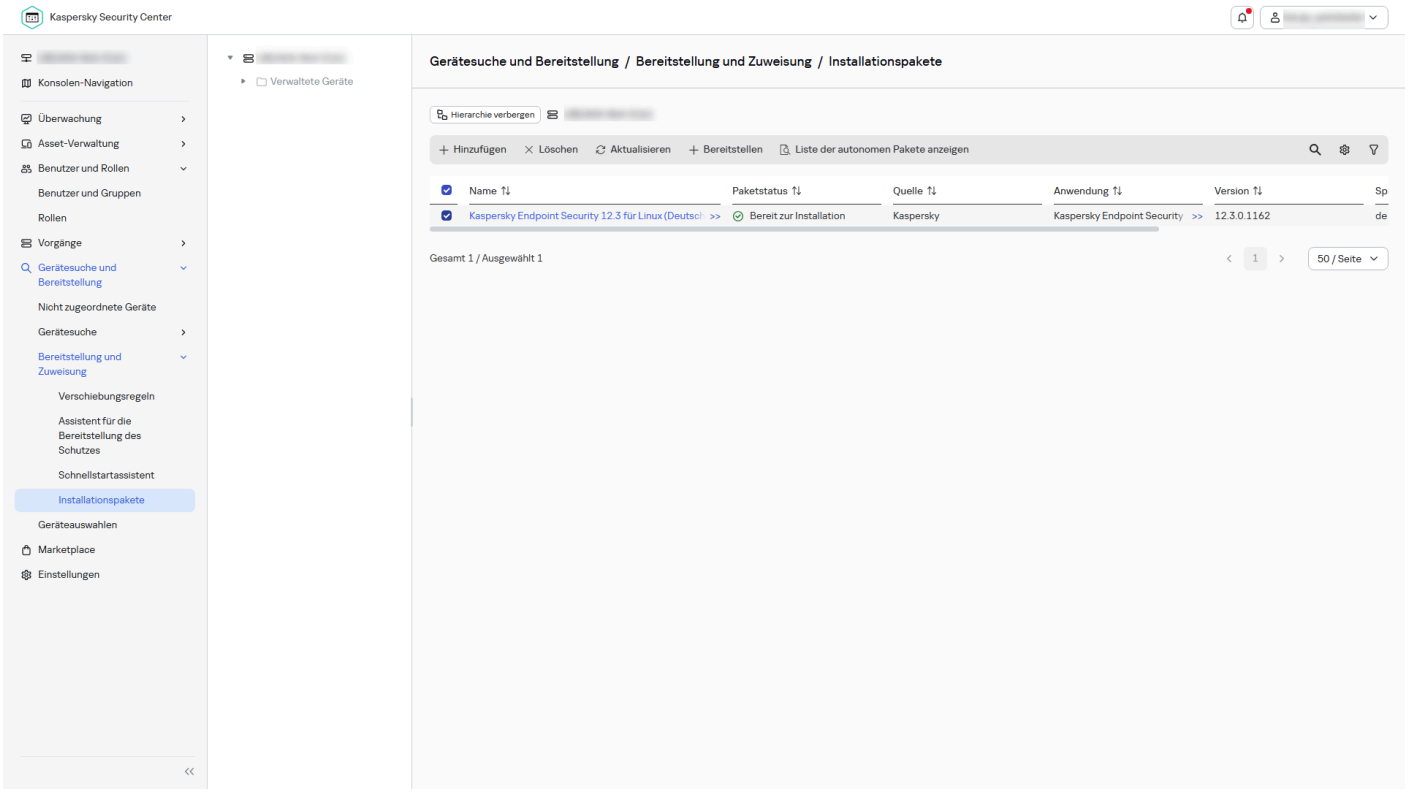
Wenn der Download-Prozess angehalten wird und sich der Status zu **EULA akzeptieren** ändert, klicken Sie auf den Namen des Installationspakets und führen Sie die Schritte 5.a und 5.b aus.

Standardmäßig werden die Installationspakete mit dem Status **In Bearbeitung** und **EULA akzeptieren** am Anfang der Liste platziert.

Wenn die Datenmenge im ausgewählten Programmpaket die aktuelle Begrenzung übersteigt, wird eine Fehlermeldung angezeigt. Sie können den Wert der Begrenzung ändern und anschließend mit der Erstellung des Installationspaketes fortfahren.

6. Wenn der Download abgeschlossen ist, klicken Sie auf die Schaltfläche **Schließen**.

Das ausgewählte Installationspaket wird in den freigegebenen Ordner des Administrationsservers in den Unterordner "Packages" heruntergeladen. Nach dem Download wird das Installationspaket in der Liste der Installationspakete angezeigt.



Die Liste der Installationspakete

Installationspakete aus einer Datei erstellen

Mit benutzerdefinierten Installationspaketen können Sie die folgenden Aufgaben ausführen:

- Um eine beliebige Anwendung (wie einen Text-Editor) auf einem Client-Gerät zu installieren, beispielsweise mithilfe einer Aufgabe.
- Zum Erstellen eines autonomen Installationspakets.

Ein benutzerdefiniertes Installationspaket ist ein Ordner mit einem Satz von Dateien. Die Quelle, aus der ein benutzerdefiniertes Installationspaket erstellt wird, ist eine *Archivdatei*. Die Archivdatei enthält eine Datei oder mehrere Dateien, die in das benutzerdefinierte Installationspaket aufgenommen werden müssen.

Wenn Sie ein benutzerdefiniertes Installationspaket erstellen, können Sie Befehlszeilenparameter angeben, z. B. um die Anwendung im Silent-Modus zu installieren.

Im Video erfahren Sie, wie Sie ein benutzerdefiniertes Installationspaket für Windows erstellen und bereitstellen. Die Textversion dieses Tutorials für Windows- und Linux-Geräte finden Sie weiter unten.

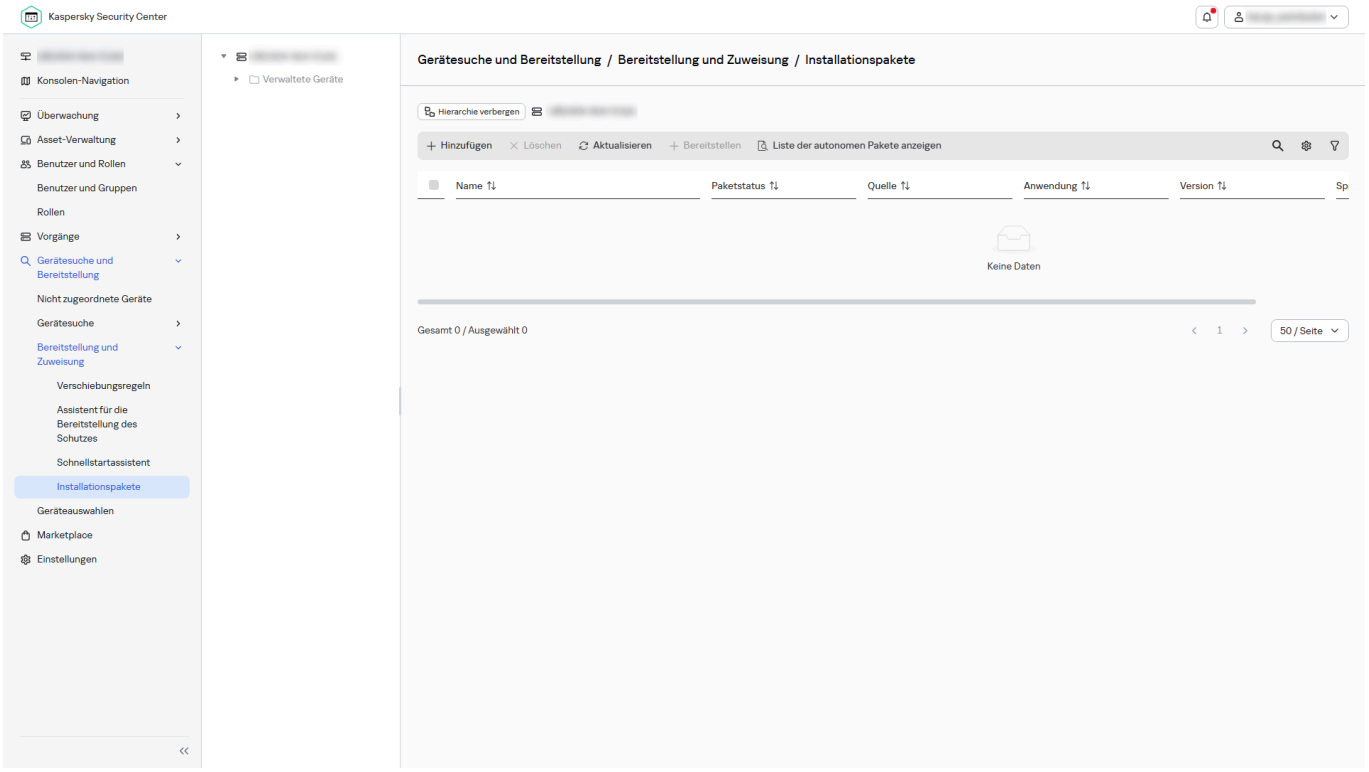


Ein benutzerdefiniertes Installationspaket für Windows aus einer Datei erstellen und bereitstellen. Videodateien

So erstellen Sie ein benutzerdefiniertes Installationspaket:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung** → **Installationspakete**.

Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

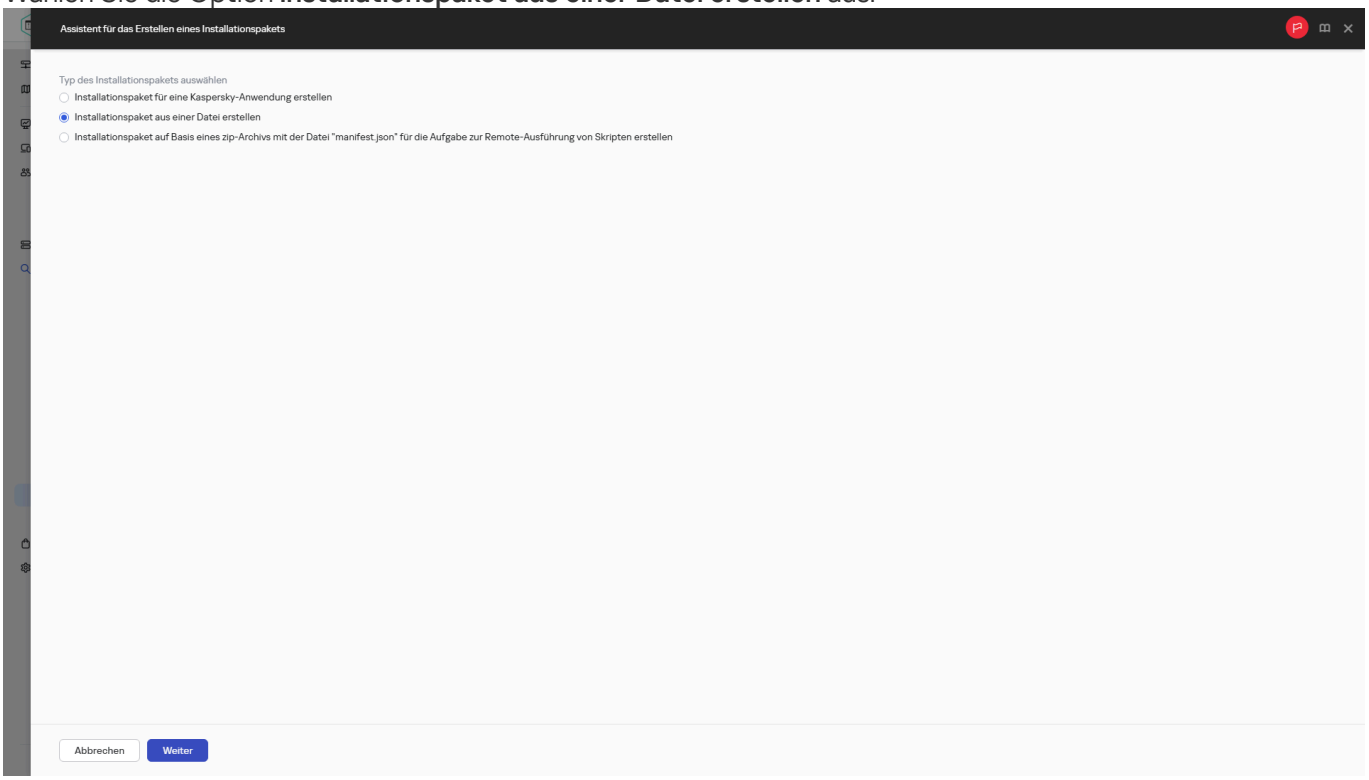


Die Liste der Installationspakete

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für neue Installationspakete wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie die Option **Installationspaket aus einer Datei erstellen** aus.



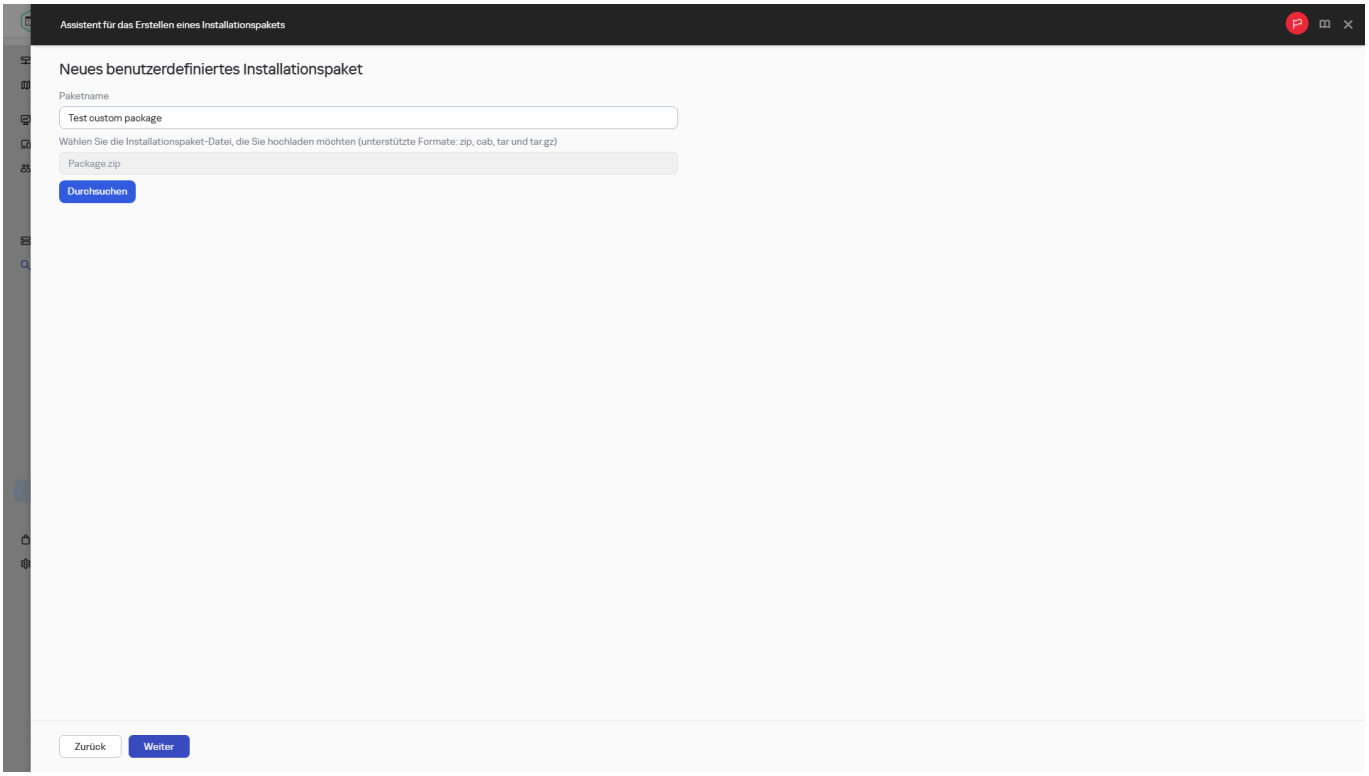
Typ des Installationspakets auswählen

4. Geben Sie den Namen des Pakets an und klicken Sie auf die Schaltfläche **Durchsuchen**.

5. Wählen Sie im angezeigten Fenster eine Archivdatei aus, die sich auf den verfügbaren Datenträgern befindet.

Sie können eine Archivdatei zip-, cab-, tar- oder tar.gz-Format hochladen. Es ist nicht möglich, ein Installationspaket aus einer sfx-Datei (selbstextrahierendes Archiv) zu erstellen.

Das Hochladen der Datei auf den Administrationsserver wird gestartet.



Angeben der Datei des Installationspakets

6. Wenn Sie die Datei einer Kaspersky-Anwendung angegeben haben, werden Sie möglicherweise aufgefordert, den Endbenutzer-Lizenzvertrag (EULA) für die Anwendung zu lesen und zu akzeptieren. Um fortzufahren, müssen Sie die EULA akzeptieren. Wählen Sie die Option **Die Bedingungen und Bestimmungen des Endbenutzer-Lizenzvertrags akzeptieren** aus, wenn Sie die Bedingungen EULA vollständig gelesen haben, und sie verstehen und akzeptieren.

   Darüber hinaus werden Sie möglicherweise aufgefordert, die Datenschutzrichtlinie zu lesen und zu akzeptieren. Um fortzufahren, müssen Sie die Datenschutzrichtlinie akzeptieren. Wählen Sie die Option **Ich akzeptiere die Datenschutzrichtlinie** nur dann aus, wenn Ihnen bewusst ist und Sie damit einverstanden sind, dass Ihre Daten so verarbeitet und (einschließlich in Drittländer) übertragen werden, wie es in der Datenschutzrichtlinie beschrieben ist.

7. Wählen Sie eine Datei aus (von der Liste der Dateien, die aus der ausgewählten Archivdatei extrahiert wurden) und geben Sie die Befehlszeilenparameter einer ausführbaren Datei an.

   Erstellen eines Installationspakets im deb- oder rpm-Format

   1. Erstellen Sie ein `.sh`-Script mit den folgenden Befehlen:

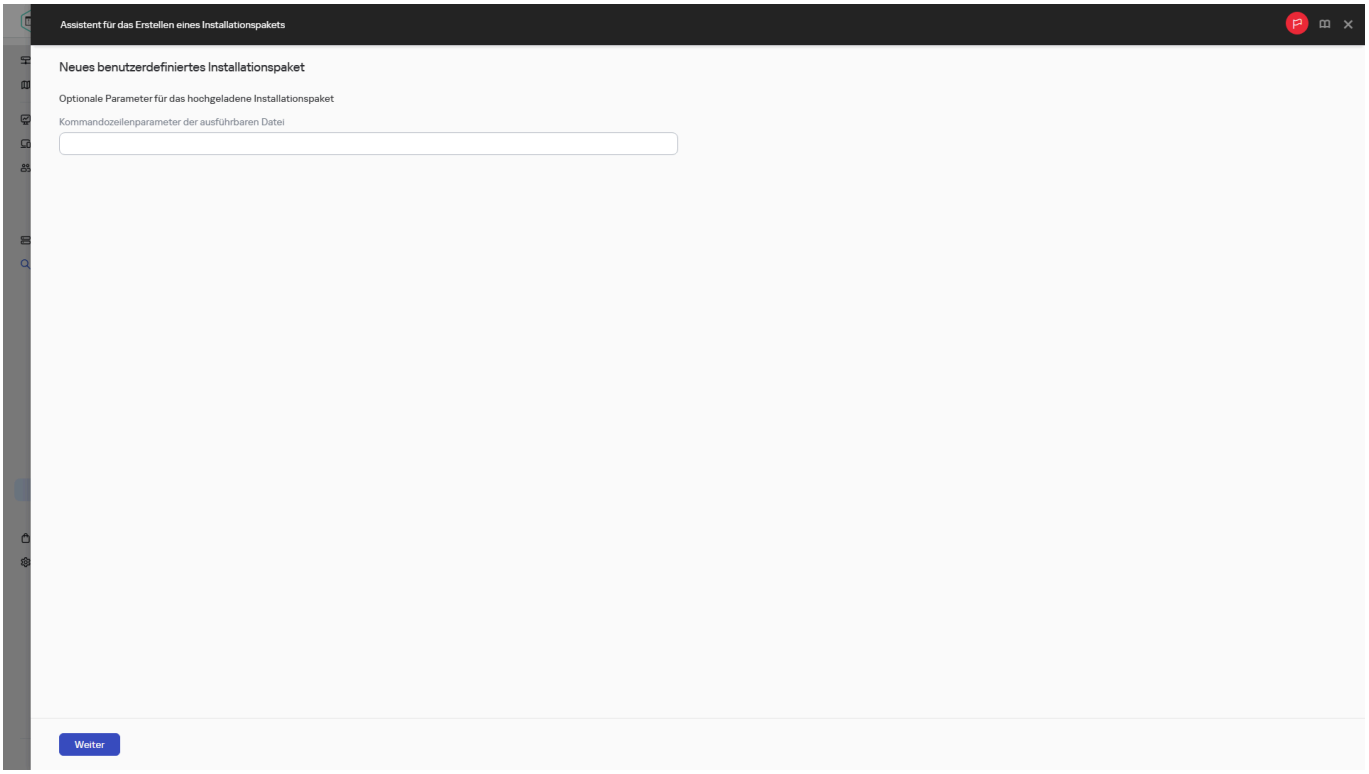
      ```
      #!/bin/sh
      script_dir="$(dirname "$0")"
      apt-get install --yes "$script_dir/<Paketname>.deb" </dev/null
      ```

      Der Inhalt und die Befehle des Skripts können je nach Paketformat und anderen Details variieren. Sie können das Skript an Ihre spezifische Konfiguration anpassen.

   2. Platzieren Sie das Skript zusammen mit der `.deb`- der `.rpm`-Datei in einem Archiv.

   3. Wählen Sie bei der Erstellung des Installationspakets das erstellte Skript als ausführbare Datei aus.

Sie können bestimmte Befehlszeilenparameter angeben, um die Anwendung im Silent-Modus aus dem Installationspaket zu installieren. Die Angabe von Befehlszeilenparametern ist optional.



Angeben der optionalen Befehlszeilenparameter

Das Erstellen des Installationspakets wird gestartet.

Der Assistent meldet, wenn der Vorgang abgeschlossen ist.

Falls das Installationspaket nicht erstellt wurde, wird eine entsprechende Meldung angezeigt.

8. Klicken Sie auf die Schaltfläche **Fertigstellen**, um den Assistenten zu schließen.

Das von Ihnen erstellte Installationspaket wird in den Unterordner "Pakete" des Freigegebenen Ordners des Administrationsservers heruntergeladen. Nach dem Herunterladen erscheint das Installationspaket in der Liste der Installationspakete.

Wenn Sie in der Liste der Installationspakete, die auf dem Administrationsserver verfügbar sind, auf den Link mit dem Namen eines benutzerdefinierten Installationspakets klicken, können Sie:

- Anzeigen der folgenden Eigenschaften eines Installationspakets:
  - **Name**. Der Name des benutzerdefinierten Installationspakets.
  - **Paketstatus**. Downloadstatus des Installationspakets.
  - **Quelle**. Der Hersteller der Anwendung.
  - **Anwendung**. Die im benutzerdefinierten Installationspaket enthaltene Anwendung.
  - **Version**. Version der Anwendung.
  - **Sprache**. Sprache der Anwendung, die im benutzerdefinierten Installationspaket enthalten ist.
  - **Größe (MB)**. Größe des Installationspakets.

- **Betriebssystem**. Typ des Betriebssystems, für welches das Installationspaket vorgesehen ist.
- **Erstellt**. Erstellungsdatum des Installationspakets.
- **Geändert**. Änderungsdatum des Installationspaketes.
- **Typ**. Typ des Installationspakets.

- Ändern Sie die Befehlszeilenparameter.

Autonome Installationspakete erstellen

Sie und die Gerätebenutzer in Ihrem Unternehmen können autonome Installationspakete verwenden, um Anwendungen manuell auf Geräten zu installieren.

Ein autonomes Installationspaket ist eine ausführbare Datei. Sie können diese Datei auf dem Webserver oder im freigegebenen Ordner speichern, per E-Mail verschicken oder auf andere Weise an ein Client-Gerät übertragen. Auf dem Client-Gerät kann der Benutzer die empfangene Datei lokal ausführen, um ohne Beteiligung von Kaspersky Security Center Linux eine Anwendung zu installieren. Sie können autonome Installationspakete für Kaspersky-Anwendungen und für Drittanbieter-Anwendungen erstellen. Um ein autonomes Installationspaket für eine Drittanbieter-Anwendung zu erstellen, müssen Sie ein benutzerdefiniertes Installationspaket erstellen.

Wenn der Administrationsserver Zugriff auf das Internet hat, wird die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers** dazu verwendet, die Abhängigkeiten herunterzuladen, die zur Erstellung des autonomen Installationspakets des Administrationsagenten erforderlich sind. Wenn der Administrationsserver keinen Zugriff auf das Internet hat, führen Sie die folgenden Schritte aus:

1. Führen Sie den folgenden Befehl aus, um das Flag "RIUtilsArchiveDirUsed" zu erstellen:

   ```
   /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n RIUtilsArchiveDirUsed -t d -v 1
   ```

2. Führen Sie den folgenden Befehl aus, um den Dienst des Administrationsservers neu zu starten:

   ```
   systemctl restart kladminserver_srv.service
   ```

3. Laden Sie die folgenden Archive von der Kaspersky-Website herunter und platzieren Sie die Archive im Ordner /var/opt/kaspersky/klnagent_srv/1093/.working/ri_utils_archives:

   - ri_utils_win32.zip
   - ri_utils_arm64.zip

   Benennen Sie die Archive nicht um.

   Der Administrationsserver verfügt nun über die erforderlichen Abhängigkeiten.

Stellen Sie sicher, dass unbefugte Personen keinen Zugriff auf das autonome Installationspaket haben.

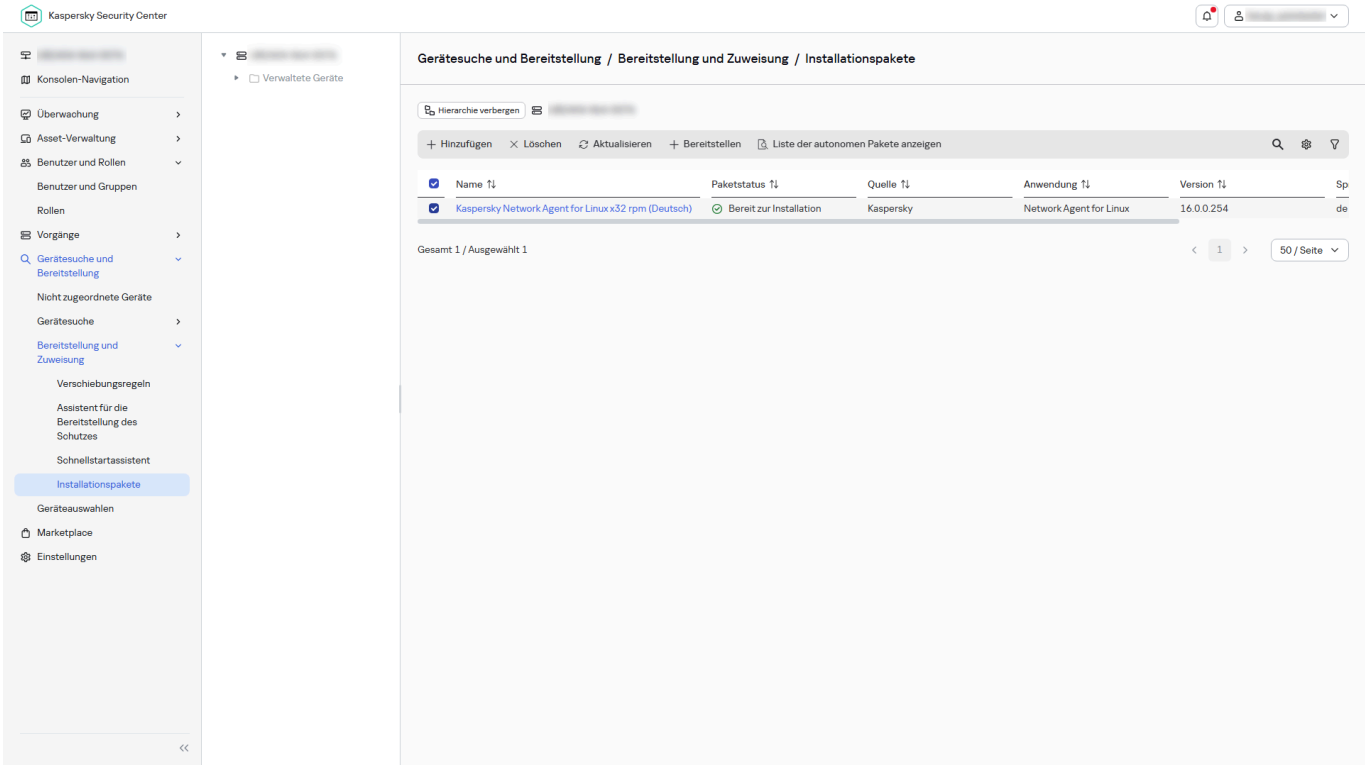
So erstellen Sie ein autonomes Installationspaket:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung** → **Installationspakete**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

Die Informationen zu Größe, Datei-Hash und Pfad sind weder in der Liste der Installationspakete für das autonome Paket des Administrationsagenten noch für alle auf virtuellen Administrationsservern erstellten Pakete verfügbar. Diese autonomen Pakete werden während des Downloads generiert.

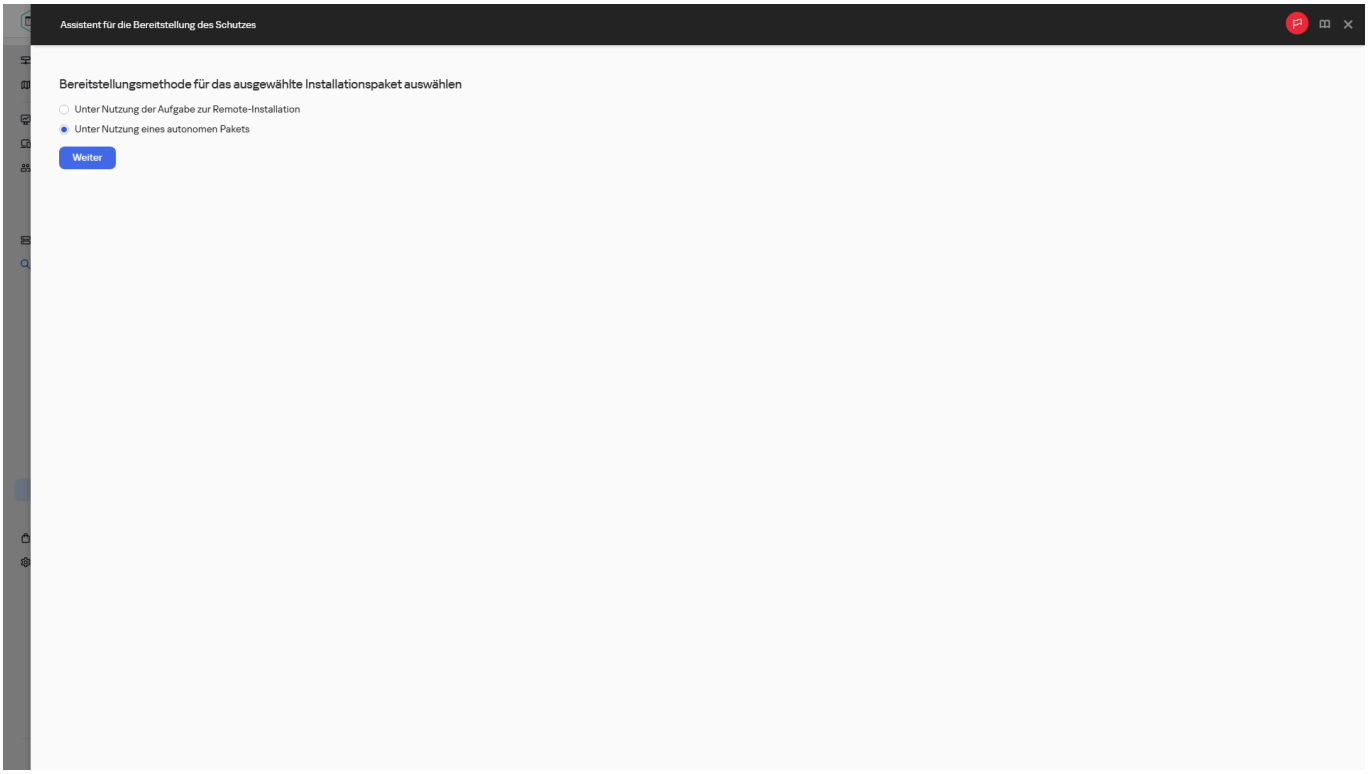
2. Wählen Sie in der Liste der Installationspakete ein Installationspaket aus und klicken Sie oberhalb der Liste auf **Bereitstellen**.



Die Liste der Installationspakete

3. Wählen Sie die Option **Unter Nutzung eines autonomen Pakets** aus.

Daraufhin wird der Assistent für das Erstellen eines autonomen Installationspakets gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.



Auswählen der Bereitstellungsmethode für das Installationspaket

4. Stellen Sie sicher, dass die Option **Administrationsagent gemeinsam mit dieser Anwendung installieren** aktiviert ist, wenn Sie den Administrationsagenten zusammen mit der ausgewählten Anwendung installieren möchten.

   Die Option wird abhängig von der Anwendung angezeigt, für die Sie ein autonomes Installationspaket erstellen.

   Diese Option ist standardmäßig aktiviert. Es wird empfohlen, diese Option zu aktivieren, wenn Sie nicht sicher sind, ob der Administrationsagent auf dem Gerät installiert ist. Falls der Administrationsagent bereits auf dem Gerät installiert ist, wird der Administrationsagent auf die neue Version aktualisiert, nachdem das autonome Installationspaket mit dem Administrationsagenten installiert wurde.

   Wenn Sie diese Option deaktivieren, wird der Administrationsagent nicht auf dem Gerät installiert und das Gerät wird nicht verwaltet.

   Falls auf dem Administrationsserver bereits ein autonomes Installationspaket für die ausgewählte Anwendung vorhanden ist, werden Sie vom Assistenten darüber informiert. In diesem Fall müssen Sie eine der folgenden Aktionen auswählen:

   - **Autonomes Installationspaket erstellen**. Wählen Sie diese Option beispielsweise dann aus, wenn Sie ein autonomes Installationspaket für eine neue Anwendungsversion erstellen und dabei ein autonomes Installationspaket beibehalten möchten, das Sie für eine ältere Anwendungsversion erstellt haben. Das neue autonome Installationspaket wird in einem anderen Ordner abgelegt.

   - **Vorhandenes autonomes Installationspaket verwenden**. Wählen Sie diese Option aus, wenn Sie ein vorhandenes autonomes Installationspaket verwenden möchten. Der Vorgang zur Paket-Erstellung wird nicht gestartet.

   - **Vorhandenes autonomes Installationspaket erneut erstellen**. Wählen Sie diese Option aus, wenn Sie ein autonomes Installationspaket für dieselbe Anwendung erneut erstellen möchten. Das autonome Installationspaket wird im selben Ordner abgelegt.

5. Standardmäßig ist im Schritt **In die Liste mit verwalteten Geräten verschieben** die Option **Geräte nicht verschieben** ausgewählt. Wenn Sie das Client-Gerät nach der Installation des Administrationsagenten nicht in Administrationsgruppen verschieben möchten, lassen Sie diese Option ausgewählt.

   Wenn Sie das Client-Gerät nach der Installation des Administrationsagenten verschieben möchten, wählen Sie die Option **Nicht zugeordnete Geräte in folgende Gruppe verschieben** aus und geben Sie die Administrationsgruppe an, in die Sie das Client-Gerät nach der Installation des Administrationsagenten verschieben möchten. Standardmäßig wird das Gerät in die Gruppe **Verwaltete Geräte** verschoben.



Auswählen der Administrationsgruppe zum Verschieben des Client-Geräts

6. Wenn die Erstellung des autonomen Installationspakets abgeschlossen ist, klicken Sie auf die Schaltfläche **Abschließen**.

   Daraufhin wird der Assistent für das Erstellen eines autonomen Installationspakets beendet.

Das autonome Installationspaket wird im Unterordner PkgInst des Freigegebenen Ordners des Administrationsservers erstellt und abgelegt. Sie können eine Liste der autonomen Pakete anzeigen. Klicken Sie dazu oberhalb der Liste der Installationspakete auf **Liste der autonomen Pakete anzeigen**.

Einstellungen des Installationspakets des Administrationsagenten

Um die Einstellungen des Installationspakets des Administrationsagenten anzupassen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung** → **Installationspakete**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Klicken Sie auf den Namen des Installationspakets für den Administrationsagenten.

Daraufhin wird das Eigenschaftenfenster des Installationspakets des Administrationsagenten geöffnet.

Die Einstellungen des Installationspakets eines Administrationsagenten sind auf den folgenden Registerkarten gruppiert:

- Registerkarte **Allgemein**

  Auf dieser Registerkarte werden die folgenden Informationen über das Installationspaket angezeigt:

  - Name des Installationspakets
  - Name und Version des Programms, für welches das Installationspaket erstellt wurde
  - Größe des Installationspakets
  - Erstellungsdatum des Installationspaketes
  - Pfad zum Speicherort des Installationspakets

- Registerkarte **Einstellungen**

  In dieser Registerkarte enthält die Einstellungen, die für die Funktionstüchtigkeit des Administrationsagenten sofort nach dessen Installation erforderlich sind.

  - Abschnitt **Einstellungen**

    - **In Standardordner installieren**

      Bei Auswahl dieser Option wird der Administrationsagent im Ordner <Datenträger>:\Programme\Kaspersky Lab\NetworkAgent installiert. Wenn dieser Ordner nicht vorhanden ist, wird er automatisch erstellt.

      Diese Variante ist standardmäßig ausgewählt.

    - **In angegebenen Ordner installieren**

      Bei Auswahl dieser Option wird der Administrationsagent im Ordner installiert, der im Eingabefeld angegeben wurde.

    - **Deinstallationskennwort verwenden**

      Wenn die Option aktiviert ist, können Sie das Kennwort für die Deinstallation des Programms angeben (nur für Administrationsagenten auf Geräten unter einem Windows-Betriebssystem verfügbar).

      Diese Option ist standardmäßig deaktiviert.

    - **Dienst des Administrationsagenten vor unberechtigter Deinstallation und Beendigung schützen sowie Änderung der Einstellungen verhindern**

      Wenn diese Option aktiviert ist, kann nach der Installation des Administrationsagenten auf einem verwalteten Gerät die Komponente nicht ohne die entsprechenden Berechtigungen entfernt oder neu konfiguriert werden. Der Dienst des Administrationsagenten kann nicht beendet werden. Diese Option hat keine Auswirkung auf Domänencontroller.

      Aktivieren Sie diese Option, um den Administrationsagenten auf Workstations zu schützen, die mit lokalen Administratorrechten betrieben werden.

      Diese Option ist standardmäßig deaktiviert.

- **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**

  Wenn diese Option aktiviert ist, werden alle heruntergeladenen Updates und Patches für den Administrationsserver, den Administrationsagenten, die Kaspersky Security Center Web Console und iOS MDM-Server automatisch installiert.

  Wenn diese Option deaktiviert ist, werden die heruntergeladenen Updates und Patches nur installiert, sobald Sie deren Status zu *Genehmigt* ändern. Updates und Patches mit dem Status *Nicht festgestellt* werden nicht installiert.

  Diese Option ist standardmäßig aktiviert.

- Abschnitt **Verbindung**

  In diesem Abschnitt können Sie die Einstellungen für die Verbindung des Administrationsagenten mit dem Administrationsserver anpassen. Zum Verbindungsaufbau können Sie das SSL- oder UDP-Protokoll verwenden. Geben Sie für die Konfiguration der Verbindung die folgenden Einstellungen an:

  - **Adresse des Administrationsservers**

    Adresse des Geräts, auf dem der Administrationsserver installiert ist.

  - **Port**

    Nummer des Ports, über den die Verbindung erfolgt.

  - **SSL-Port**

    Nummer des Ports, über den die Verbindung mit dem SSL-Protokoll erfolgt.

  - **Zertifikat des Servers verwenden**

    Wenn diese Option aktiviert ist, wird für die Authentifizierung des Zugriffs des Administrationsagenten auf den Administrationsserver eine Zertifikatsdatei verwendet, die über die Schaltfläche **Zertifikatdatei auswählen** angegeben werden kann.

    Wenn diese Option deaktiviert ist, wird die Zertifikatsdatei bei der ersten Verbindung des Administrationsagenten über die Adresse, die im Feld **Adresse des Administrationsservers** angegeben ist, vom Administrationsserver abgerufen.

    Es wird nicht empfohlen, das Kontrollkästchen zu deaktivieren, da das automatische Abrufen des Zertifikats des Administrationsservers durch den Administrationsagenten bei der Verbindung mit dem Server unsicher ist.

    Diese Option ist standardmäßig deaktiviert.

  - **SSL-Verbindung verwenden**

    Wenn diese Option aktiviert ist, erfolgt die Verbindung zum Administrationsserver über einen gesicherten Port mit SSL-Protokoll.

    Diese Option ist standardmäßig deaktiviert. Wir empfehlen, diese Option nicht zu deaktivieren, damit Ihre Verbindung gesichert bleibt.

  - **UDP-Port verwenden**

    Wenn diese Option aktiviert ist, erfolgt die Verbindung zwischen dem Administrationsagenten und dem Administrationsserver über den UDP-Port. Dies ermöglicht es, Client-Geräte zu verwalten und Informationen über sie zu erhalten.

    Der UDP-Port, der auf verwalteten Geräten mit installiertem Administrationsagent geöffnet sein muss. Daher empfehlen wir, diese Option nicht zu deaktivieren.

Diese Option ist standardmäßig aktiviert.

- **UDP-Port**

  In diesem Feld kann der Port zur Verbindung des Administrationsservers mit dem Administrationsagenten mittels UDP-Protokoll angegeben werden.

  Standardmäßig wird die Nummer des UDP-Ports 15000 verwendet.

- **Keinen Proxyserver verwenden**

  Wenn diese Option aktiviert ist, wird die direkte Verbindung genutzt, um das Gerät mit dem Administrationsserver zu verbinden.

- **Proxyserver verwenden**

  Wenn diese Option aktiviert ist, geben Sie die Parameter des Proxyservers an:

  - **Proxyserver-Adresse**
  - **Proxyserver-Port**

  Falls Ihr Proxyserver eine Authentifizierung erfordert, aktivieren Sie die Option **Authentifizierung am Proxyserver** und geben Sie den **Benutzername** und das **Kennwort** für das Konto ein, unter dem die Verbindung mit dem Proxyserver hergestellt wird. Es wird empfohlen, dass Sie die Anmeldeinformationen für ein Konto angeben, das lediglich über die Mindestberechtigungen verfügt, die für die Proxyserver-Authentifizierung erforderlich sind.

- **Ports des Administrationsagenten in der Windows-Firewall öffnen**

  Wenn diese Option aktiviert ist, werden die von Network Agent verwendeten Ports zur Ausschlussliste der Microsoft Windows Firewall hinzugefügt.

  Diese Option ist standardmäßig aktiviert.

  > Diese Option ist nur für Installationspakete des Administrationsagenten verfügbar, die für Windows-Geräte vorgesehen sind.

- Abschnitt **Erweitert**

  In diesem Abschnitt können Sie die Verwendung des Verbindungs-Gateways konfigurieren.

  In der Einstellungsgruppe **Verbindungs-Gateway** können Sie die Verbindungsmethode zwischen einem Gerät und dem Administrationsserver konfigurieren:

  - **Administrationsagent als Verbindungs-Gateway in der DMZ verwenden**

    Wenn diese Option aktiviert ist, wird der Administrationsagenten als Verbindungsgateway in der demilitarisierten Zone (DMZ) verwendet, um eine Verbindung zum Administrationsserver herzustellen, mit ihm zu kommunizieren und während der Datenübertragung die Daten auf dem Administrationsagenten sicher aufzubewahren.

  - **Eine Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen**

    Wenn diese Option aktiviert ist, wird die Verbindung zum Administrationsserver unter Verwendung eines Verbindung-Gateways hergestellt, um die Anzahl der Verbindungen zum Administrationsserver zu reduzieren. Geben Sie in diesem Fall im Feld **Adresse des Verbindungs-Gateways** die Adresse des Geräts ein, das als Verbindungs-Gateway fungieren soll.

In der Einstellungsgruppe **Virtuelle Maschine** können Sie die Verbindung für Virtual Desktop Infrastructure (VDI) konfigurieren, wenn Ihr Netzwerk virtuelle Maschinen umfasst:

- **Dynamischen Modus für VDI aktivieren**

  Wenn diese Option aktiviert ist, wird für den auf einer virtuellen Maschine installierten Administrationsagenten der dynamische Modus Virtual Desktop Infrastructure (VDI) aktiviert.

  Diese Option ist standardmäßig deaktiviert.

- **Einstellungen für VM optimieren**

  Wenn diese Option aktiviert ist, sind in den Einstellungen des Administrationsagenten folgende Funktionen deaktiviert:

  - Informationen über die installierte Software empfangen
  - Informationen über die Hardware empfangen
  - Informationen über vorhandene Schwachstellen empfangen
  - Informationen über erforderliche Updates empfangen

  Diese Option ist standardmäßig deaktiviert.

Wenn Sie möchten, dass nach der Installation des Administrationsagenten auf Linux-Geräten die Benutzer automatisch aufgefordert werden, sich als Gerätebesitzer anzumelden, aktivieren Sie die Option **Ausführen des Tools zur Benutzerregistrierung nach Installation des Administrationsagenten zulassen**.

Wenn diese Option aktiviert ist, wird nach der Installation des Administrationsagenten ein Tool ausgeführt, das den Benutzer als Gerätebesitzer registriert. Diese Option ist standardmäßig deaktiviert.

- Abschnitt **Tags**

  Im Abschnitt **Tags** wird eine Liste mit Schlüsselwörtern (Tags) angezeigt, die Client-Geräten zugewiesen werden können, nachdem der Administrationsagent auf ihnen installiert wurde. Sie können Tags aus der Liste hinzufügen und löschen sowie Tags umbenennen.

  Wenn das Kontrollkästchen neben einem Tag aktiviert ist, wird das Tag bei der Installation des Administrationsagenten automatisch zum entsprechenden verwalteten Gerät hinzugefügt.

  Ist das Kontrollkästchen neben einem Tag deaktiviert, wird das Tag bei der Installation des Administrationsagenten nicht automatisch zum verwalteten Gerät hinzugefügt. Dieses Tag kann manuell zu Geräten hinzugefügt werden.

  Wird ein Tag aus der Liste gelöscht, so wird dieses Tag automatisch auf allen Geräten deaktiviert, zu denen es hinzugefügt wurde.

  > Regeln für das automatische Zuweisen von Tags werden nicht von Installationspaketen des Administrationsagenten angewendet, die für Linux- oder macOS-Geräte bestimmt sind.

- Registerkarte **Autonome Pakete**

  Auf dieser Registerkarte haben Sie Möglichkeiten zum:

  - Anzeigen der Liste der verfügbaren autonomen Installationspakete
  - Veröffentlichen eines autonomen Installationspakets auf dem "Web Server" durch Klick auf **Veröffentlichen**. Ein veröffentlichtes autonomes Installationspaket kann von jenen Benutzern heruntergeladen werden, denen Sie einen Link für dieses autonome Installationspaket geschickt haben.

- Aufheben der Veröffentlichung eines autonomen Installationspakets auf dem "Web Server" durch Klick auf **Veröffentlichung aufheben**. Ein unveröffentlichtes autonomes Installationspaket kann nur von Ihnen selbst und von anderen Administratoren heruntergeladen werden.

- Herunterladen eines autonomen Installationspakets auf Ihr Gerät, indem Sie auf die Schaltfläche **Herunterladen** klicken.

- Senden einer E-Mail-Nachricht mit einem Link für das autonome Installationspaket durch Klick auf **Per E-Mail senden**.

- Löschen Sie ein autonomes Installationspaket, indem Sie auf die Schaltfläche **Entfernen** klicken.

- Registerkarte **Revisionsverlauf**

  Auf dieser Registerkarte können Sie den Revisionsverlauf des Installationspakets anzeigen. Sie können Revisionen vergleichen, Revisionen ansehen, Revisionen in einer Datei speichern und Beschreibungen von Revisionen hinzufügen und ändern.

Von Kaspersky Security Center Linux erstellte autonomen Pakete ausführen

Die oben beschriebenen Methoden zur erstmaligen Bereitstellung des Administrationsagenten und der Apps können möglicherweise nicht immer durchgeführt werden, da nicht immer alle notwendigen Bedingungen erfüllt werden können. In solchen Fällen kann aus den vom Administrator vorbereiteten Installationspaketen mit den notwendigen Installationseinstellungen mithilfe von Kaspersky Security Center Linux eine einheitliche ausführbare Datei erstellt werden, die als *autonomes Installationspaket* bezeichnet wird. Ein autonomes Installationspaket kann sowohl auf einem internen Webserver (in Kaspersky Security Center Linux enthalten) veröffentlicht werden, sofern dies angebracht ist (d. h. wenn die Gerätebenutzer Zugriff auf diesen Webserver von außen haben), als auch auf einem speziell bereitgestellten Webserver, der in Kaspersky Security Center Web Console enthalten ist. Die autonomen Pakete können auch auf einen anderen Webserver kopiert werden.

Mithilfe von Kaspersky Security Center Linux kann ausgewählten Benutzern per E-Mail ein Link zur Datei des autonomen Pakets auf dem verwendeten Webserver mit der Bitte gesendet werden, die Datei auszuführen (interaktiv oder mit dem Parameter "-s" für die "Silent"-Installation). Das autonome Installationspaket kann für Benutzer von Geräten, die keinen Zugriff auf den Webserver haben, an eine E-Mail-Nachricht angehängt werden. Der Administrator kann das autonome Paket auf einen Wechseldatenträger kopieren, es an das relevante Gerät liefern und dann später ausführen.

Das autonome Paket kann aus dem Paket des Administrationsagenten, dem Paket anderer Apps (beispielsweise der Sicherheitsanwendung) oder sofort aus beiden Paketen erstellt werden. Wenn das autonome Paket aus dem Administrationsagenten und aus anderen Apps erstellt wurde, beginnt die Installation mit dem Administrationsagenten.

Beim Erstellen des autonomen Paketes mit dem Administrationsagenten kann die Administrationsgruppe angegeben werden, in welche die neuen Geräte (kein Bestandteil der Administrationsgruppen) automatisch nach Abschluss der Installation des Administrationsagenten verschoben werden.

Die autonomen Pakete können interaktiv (standardmäßig), mit Anzeige des Installationsergebnisses der zugehörigen Apps oder im Silent-Modus (beim Start mit dem Parameter "-s") ausgeführt werden. Der Silent-Modus kann für die Installation aus bestimmen Skripts (beispielsweise aus Skripts, die für den Start nach Abschluss der Bereitstellung des Betriebssystem-Images angepasst werden, und ähnliches) verwendet werden. Das Installationsergebnis des Silent-Modus wird durch den Rückgabecode des Prozesses definiert.

Programme mithilfe autonomer Installationspakete installieren

Kaspersky Security Center ermöglicht das Erstellen von autonomen Installationspaketen für Programme. Ein autonomes Installationspaket ist eine ausführbare Datei, die auf einem Webserver abgelegt, per E-Mail verschickt oder auf andere Weise auf ein Client-Gerät übertragen werden kann. Die empfangene Datei kann lokal auf dem Client-Gerät gestartet werden, um das Programm ohne Beteiligung von Kaspersky Security Center zu installieren.

So installieren Sie eine Anwendung unter Verwendung eines autonomen Installationspakets:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung → Installationspakete**.
2. Aktivieren Sie das Kontrollkästchen neben dem Installationspaket der gewünschten Anwendung und klicken Sie anschließend auf die Schaltfläche **Bereitstellen**.
3. Wählen Sie im neuen Fenster die Option **Unter Nutzung eines autonomen Pakets** aus und klicken Sie anschließend auf die Schaltfläche **Weiter**.

   Daraufhin wird der Assistent für das Erstellen eines autonomen Installationspakets gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
4. Wählen Sie die Option **Autonomes Installationspaket erstellen** aus.
5. Geben Sie an, ob die Geräte nach Abschluss der Installation des Administrationsagenten in die Administrationsgruppe verschoben werden müssen.
6. Wählen Sie im letzten Schritt des Assistenten eine Methode zum Übertragen des autonomen Installationspakets auf das Client-Gerät und klicken Sie anschließend auf die Schaltfläche **Fertigstellen**, um den Assistenten zu beenden.
7. Übertragen Sie das autonome Installationspaket für das Programm auf das Client-Gerät.
8. Starten Sie das autonome Installationspaket auf dem Client-Gerät.

   Daraufhin wird das Programm auf dem Client-Gerät mit den Einstellungen installiert, die im autonomen Paket vorgegeben wurden.

Beim Erstellen wird ein autonomes Installationspaket automatisch auf dem Webserver veröffentlicht. Der Link für den Download des autonomen Paketes wird in der Liste der erstellten autonomen Installationspakete angezeigt. Bei Bedarf können Sie die Veröffentlichung des gewählten autonomen Paketes abbrechen und es erneut auf dem Webserver veröffentlichen. Standardmäßig wird für den Download der autonomen Installationspakete Port 8060 verwendet.

Zweckdienlichkeit des Datenbanken-Updates im Installationspaket der Sicherheitsanwendung

Vor Beginn der Bereitstellung des Schutzes muss die Möglichkeit eines Updates der Antiviren-Datenbanken (einschließlich der Autopatch-Module), die zusammen mit dem Programmpaket der Sicherheitsanwendung bereitgestellt werden, berücksichtigt werden. Es ist zweckmäßig, vor Beginn der Bereitstellung die Datenbanken aus dem Bestand des Installationspakets der App (beispielsweise mithilfe des entsprechenden Befehls im Kontextmenü des ausgewählten Installationspakets) zu aktualisieren. Dadurch wird die Anzahl der Neustarts verringert, die für den Abschluss der Bereitstellung des Schutzes auf den Geräten erforderlich sind.

Größenbegrenzung für benutzerdefinierte Installationspakete anpassen

Die Gesamtgröße der während der Erstellung eines benutzerdefinierten Installationspakets entpackten Daten ist begrenzt. Das Standardlimit beträgt 1 GB.

Wenn Sie versuchen ein Archiv hochzuladen, dessen beinhalteten Daten die aktuelle Begrenzung übersteigen, wird eine Fehlermeldung angezeigt. Wenn Sie Installationspakete aus großen Programmpaketen erstellen, müssen Sie unter Umständen den Grenzwert erhöhen.

Um den Grenzwert für benutzerdefinierte Installationspakete zu ändern:

1. Führen Sie auf dem Gerät des Administrationsservers die Eingabeaufforderung unter dem Konto aus, dass verwendet wurde, um den Administrationsserver zu installieren.

2. Ändern Sie das aktuelle Verzeichnis des Installationsordners von Kaspersky Security Center Linux (üblicherweise /opt/kaspersky/ksc64/sbin).

3. Geben Sie je nach Art der Installation des Administrationsservers einen der folgenden Befehle unter einem Benutzerkonto mit Root-Rechten ein:

   - Gewöhnliche lokale Installation:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <Anzahl an Bytes>
     ```

   - Installation auf einem Kaspersky Security Center Linux Failover-Cluster:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <Anzahl an Bytes> --stp klfoc
     ```

   Wobei <Anzahl an Bytes> eine Anzahl an Bytes im Hexadezimal- oder Dezimalformat ist.

   Wenn das erforderliche Limit beispielsweise 2 GB beträgt, können Sie den Dezimalwert 2147483648 oder den Hexadezimalwert 0x80000000 angeben. In diesem Fall können Sie für eine lokale Installation des Administrationsservers den folgenden Befehl verwenden:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Die Größenbegrenzung für benutzerdefinierte Installationspakete wird geändert.

Installationspakete an sekundäre Administrationsserver verteilen

Kaspersky Security Center Linux ermöglicht Ihnen das erstellen von Installationspaketen für Kaspersky-Anwendungen und für Anwendungen von Drittanbietern. Darüber hinaus können Sie die Installationspakete an Client-Geräte verteilen und Anwendungen aus den Paketen installieren. Um die Auslastung des primären Administrationsservers zu optimieren, können Sie Installationspakete auf sekundäre Administrationsserver verteilen. Danach übertragen die sekundären Server die Pakete an die Client-Geräte, und anschließend können Sie die Remote-Installation der Anwendungen auf Ihren Client-Geräten durchführen.

Um Installationspakete auf sekundäre Administrationsserver zu verteilen:

1. Stellen Sie sicher, dass die sekundären Administrationsserver mit dem primären Administrationsserver verbunden sind.

2. Wechseln Sie im Hauptmenü zu **Aufgaben**.

   Die Aufgabenliste wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.

4. Wählen Sie auf der Seite **Einstellungen der neue Aufgabe** in der Dropdown-Liste **Anwendung** die Option **Kaspersky Security Center**. Wählen Sie anschließend von der Dropdown-Liste **Aufgabentyp** die Option **Installationspaket verteilen** aus und geben Sie den Aufgabennamen an.

5. Wählen Sie auf der Seite **Gültigkeitsbereich der Aufgabe** die Geräte aus, denen die Aufgabe auf folgende Arten zugewiesen ist:

   - Wenn Sie eine Aufgabe für alle sekundären Administrationsserver einer bestimmten Administrationsgruppe erstellen möchten, wählen Sie diese Gruppe aus und erstellen Sie anschließend eine Gruppenaufgabe für sie.

   - Wenn Sie eine Aufgabe für bestimmte sekundäre Administrationsserver erstellen möchten, wählen Sie diese Server aus und erstellen Sie anschließend eine Aufgabe für diese.

6. Wählen Sie auf der Seite **Verteilte Installationspakete** die Installationspakete aus, die auf die sekundären Administrationsserver kopiert werden sollen.

7. Geben Sie ein Konto an, unter dem die Aufgabe *Installationspaket verteilen* ausgeführt wird. Sie können Ihr Konto verwenden und die Option **Standardbenutzerkonto** aktiviert lassen. Alternativ können Sie angeben, dass die Aufgabe unter einem anderen Konto ausgeführt werden soll, welches über die erforderlichen Zugriffsrechte verfügt. Wählen Sie dazu die Option **Benutzerkonto festlegen** aus und geben Sie anschließend die Anmeldeinformationen für dieses Konto ein.

8. Auf der Seite **Erstellung der Aufgabe abschließen** können Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, um anschließend das Fenster mit den Aufgabeneigenschaften zu öffnen und die Aufgabeneinstellungen zu ändern. Alternativ können Sie Aufgabeneinstellungen jederzeit später konfigurieren.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Die Aufgabe, die zur Verteilung der Installationspakete an die sekundären Administrationsserver erstellt wurde, wird in der Aufgabenliste angezeigt.

10. Sie können die Aufgabe manuell starten oder warten, bis die Aufgabe nach dem in den Aufgabeneinstellungen festgelegten Zeitplan gestartet wird.

Nach Abschluss der Aufgabe werden die ausgewählten Installationspakete auf die angegebenen sekundären Administrationsserver kopiert.

Liste der autonomen Installationspakete anzeigen

Sie können die Liste der autonomen Installationspakete und die Eigenschaften jedes der autonomen Installationspakete anzeigen.

So zeigen Sie die Liste der autonomen Installationspakete für alle Installationspakete an:

Klicken Sie oberhalb der Liste auf die Schaltfläche **Liste der autonomen Pakete anzeigen**.

In der Liste der autonomen Installationspakete werden deren Eigenschaften wie folgt angezeigt:

- **Paketname**. Name des autonomen Installationspaketes, der automatisch aus dem Namen der im Paket enthaltenen Anwendung und der Anwendungsversion gebildet wird.
- **Anwendungsname**. Name der Anwendung, die in dem autonomen Installationspaket enthalten ist.
- **Anwendungsversion**.
- **Installationspaket-Name des Administrationsagenten**. Diese Eigenschaft wird nur angezeigt, wenn in dem autonomen Installationspaket der Administrationsagent enthalten ist.
- **Version des Administrationsagenten**. Diese Eigenschaft wird nur angezeigt, wenn in dem autonomen Installationspaket der Administrationsagent enthalten ist.
- **Größe**. Dateigröße (MB).
- **Gruppe**. Name der Gruppe, in die das Client-Gerät nach der Installation des Administrationsagenten verschoben wird.
- **Erstellt**. Datum und Uhrzeit der Erstellung des autonomen Installationspakets.
- **Geändert**. Datum und Uhrzeit der Änderung des autonomen Installationspakets.
- **Pfad**. Vollständiger Pfad des Ordners, in dem sich das autonome Installationspaket befindet.
- **Webadresse**. Webadresse des Speicherorts für das autonome Installationspaket.
- **Datei-Hash**. Mit dieser Eigenschaft wird bestätigt, dass das autonome Installationspaket nicht von Dritten geändert wurde und der Benutzer dieselbe Datei erhalten hat, die Sie erstellt und an den Benutzer übertragen haben.

Die Informationen zu Größe, Datei-Hash und Pfad sind weder in der Liste der Installationspakete für das autonome Paket des Administrationsagenten noch für alle auf virtuellen Administrationsservern erstellten Pakete verfügbar. Diese autonomen Pakete werden während des Downloads generiert.

So zeigen Sie die Liste der autonomen Installationspakete für ein bestimmtes Installationspaket an:

Wählen Sie in der Liste das Installationspaket aus und klicken Sie auf die Schaltfläche **Liste der autonomen Pakete anzeigen** über der Liste.

In der Liste der autonomen Installationspakete können Sie Folgendes tun:

- Veröffentlichen eines autonomen Installationspakets auf dem "Web Server" durch Klick auf **Veröffentlichen**. Ein veröffentlichtes autonomes Installationspaket kann von jenen Benutzern heruntergeladen werden, denen Sie einen Link für dieses autonome Installationspaket geschickt haben.
- Aufheben der Veröffentlichung eines autonomen Installationspakets auf dem "Web Server" durch Klick auf **Veröffentlichung aufheben**. Ein unveröffentlichtes autonomes Installationspaket kann nur von Ihnen selbst und von anderen Administratoren heruntergeladen werden.

- Herunterladen eines autonomen Installationspakets auf Ihr Gerät, indem Sie auf die Schaltfläche **Herunterladen** klicken.
- Senden einer E-Mail-Nachricht mit einem Link für das autonome Installationspaket durch Klick auf **Per E-Mail senden**.
- Löschen Sie ein autonomes Installationspaket, indem Sie auf die Schaltfläche **Entfernen** klicken.

Administrationsagent für Linux installieren

Zur Verwaltung der Unternehmensgeräte muss auf den Geräten der Administrationsagent installiert werden. Die Bereitstellung eines verteilten Kaspersky Security Center Linux auf den Geräten des Unternehmens beginnt gewöhnlich mit der Installation des Administrationsagenten.

Die folgenden Methoden stehen zur erstmaligen Installation des Administrationsagenten auf einem verwalteten Linux-Gerät zur Verfügung:

- Mittels SSH-Verbindung zum verwalteten Gerät und der Ausführung der Aufgabe zur Remote-Installation.
- Durch Ausführen der Paketinstallation auf dem verwalteten Gerät.

Nachdem der Administrationsagent auf einem Gerät installiert wurde, können Sie auf diesem Gerät mittels Administrationsagent die Remote-Installation von Kaspersky-Anwendungen durchführen. Dabei wird die Übertragung des Programmpakets der zu installierenden App zusammen mit den vom Administrator festgelegten Installationseinstellungen über die Verbindungskanäle zwischen den Administrationsagenten und dem Administrationsserver durchgeführt. Für die Übertragung des Programmpakets können Sie Knoten zur weiteren Verteilung in Form von Verteilungspunkten, Multicast-Versand usw. verwendet werden.

Bei der Auswahl von Methode und Strategie zur Bereitstellung der Programme im verwalteten Netzwerk muss eine Reihe von Faktoren beachtet werden (unvollständige Liste):

- Konfiguration des Unternehmensnetzwerks.
- Gesamtzahl der Geräte.
- Im Unternehmensnetzwerk vorhandene Geräte, die nicht Mitglieder der Domänen sind, und vorhandene einheitliche Benutzerkonten mit Administratorrechten auf solchen Geräten.
- Breite des Kanals zwischen dem Administrationsserver und den Geräten.
- Charakter der Verbindung zwischen dem Administrationsserver und den Remote-Subnetzen sowie Breite der Netzwerkkanäle innerhalb solcher Subnetze.
- Sicherheitseinstellungen, die zu Beginn der Bereitstellung auf Remote-Geräten angewendet wurden. Mit diesen Parametern kann eine Remote-Verbindung zu dem verwalteten Gerät hergestellt und der Installer gestartet werden.

Ein Gerät mit Linux-Betriebssystem für die Installation des Administrationsagenten vorbereiten

Bevor Sie den Administrationsagenten auf einem Linux-Gerät installieren können, müssen Sie einige vorbereitende Schritte ausführen, die für jedes Linux Gerät erforderlich sind.

Um ein Gerät mit dem Betriebssystem Linux für die Remote-Installation des Administrationsagenten vorzubereiten, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass auf dem Gerät, auf dem Sie den Administrationsagenten für Linux installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

2. Wenn Sie Administrationsagent unter AltOS im Modus „Geschlossene Softwareumgebung“ installieren möchten, deaktivieren Sie den Modus „Geschlossene Softwareumgebung“, bis die Installation abgeschlossen ist.

3. Laden Sie das Installationspaket des Administrationsagenten über die Benutzeroberfläche der Web Console oder von der Kaspersky-Website herunter.

   Wenn Sie den Administrationsagenten auf einem Linux-System mit der glibc-Version 2.5 installieren, müssen Sie das Installationspaket des *Kaspersky-Administrationsagenten für Legacy-Linux-Systeme* verwenden. Sie können das Paket über die Benutzeroberfläche der Web Console oder von der Kaspersky-Website herunterladen.

4. Stellen Sie sicher, dass auf dem Linux-Zielgerät die folgende Software installiert ist:

   - Sudo (für Ubuntu 10.04 ist Sudo ab Version 1.7.2p1 erforderlich)
   - Perl-Sprachinterpreter ab Version 5.10
   - ps-Tool

5. Testen Sie die Konfiguration des Geräts:

   a. Stellen Sie sicher, dass eine Verbindung zum Gerät über ein Client-Programm mit SSH möglich ist (z. B. PuTTY).

      Wenn Sie keine Verbindung zum Gerät herstellen können, öffnen Sie die Datei `/etc/ssh/sshd_config` und stellen Sie sicher, dass die folgenden Einstellungen die nachstehenden Werte besitzen:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      Ändern Sie die Datei /etc/ssh/sshd_config nicht, wenn Sie sich problemlos mit dem Gerät verbinden können. Andernfalls kann es zu einem Fehler bei der SSH-Authentifizierung kommen, wenn eine Aufgabe zur Remote-Installation ausgeführt wird.

      Speichern Sie die Datei (bei Bedarf) und starten Sie den SSH-Dienst über den Befehl `sudo service ssh restart` neu.

b. Stellen Sie sicher, dass auf einem Linux-basierten nicht zugewiesenen Gerät der TCP-Port 22 erreichbar und geöffnet ist.

Um den Administrationsagenten für Linux installieren zu können, muss der TCP-Port 22 verfügbar sein.

c. Deaktivieren Sie das Kennwort der sudo-Abfrage für das Benutzerkonto, das für die Verbindung mit dem Gerät verwendet wird.

d. Verwenden Sie den Befehl `visudo` in sudo, um die Konfigurationsdatei sudoers zu öffnen.

Fügen Sie der geöffneten Datei am Ende die folgende Zeile hinzu: `<Benutzername> > ALL = (ALL) NOPASSWD: ALL`. In diesem Fall ist `< Benutzername >` ein Benutzerkonto, das für die Verbindung mit dem Gerät über das SSH-Protokoll verwendet wird. Wenn Sie das Betriebssystem Astra Linux verwenden, fügen Sie am Ende der Datei "/etc/sudoers" die Zeile mit dem folgenden Text an: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

e. Speichern und schließen Sie die Datei sudoers.

f. Stellen Sie erneut eine Verbindung zum Gerät über SSH her und stellen Sie mithilfe des Befehls `sudo whoami` sicher, dass der Sudo-Dienst kein Kennwort abfragt.

6. Wenn Sie den Administrationsagenten auf Geräten remote installieren möchten, auf denen ein Betriebssystem mit dem Initialisierungssystem "systemd" ausgeführt wird, öffnen Sie die Datei `/etc/systemd/logind.conf` und führen Sie einen der folgenden Schritte aus:

- Geben Sie für die Einstellung `KillUserProcesses` den Wert `no` an: `KillUserProcesses=no`.
- Geben Sie für die Einstellung `KillExcludeUsers` den Benutzernamen des Kontos an, unter dem die Remote-Installation durchgeführt wird, z. B. `KillExcludeUsers=root`.

Zielgerät mit Astra Linux

Wenn auf dem Zielgerät Astra Linux ausgeführt wird, fügen Sie die Zeichenfolge export `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` in die Datei `/home/< Benutzername >/.bashrc` ein, wobei `< Benutzername >` für jenes Benutzerkonto steht, das für die Geräteverbindung über SSH verwendet werden soll.

Zielgerät mit OSnova

Wenn auf dem Zielgerät OSnova ausgeführt wird, gehen Sie wie folgt vor:

a. Öffnen Sie die Datei `/usr/lib/systemd/logind.conf/10-enable-kill-user-processes.conf` und kommentieren Sie anschließend die Zeile `#KillUserProcess=yes` aus.

b. Öffnen Sie die Datei `/usr/lib/NESS/pam-user-session` und kommentieren Sie anschließend die Zeile `#loginctl terminate-session "$XDG_SESSION_ID"` aus.

Um die geänderten Einstellungen zu übernehmen, starten Sie das Linux-Gerät neu oder führen Sie den folgenden Befehl aus:

```
sudo systemctl restart systemd-logind.service
```

7. Wenn Sie den Administrationsagenten auf Geräten mit dem Betriebssystem SUSE Linux Enterprise Server 15 installieren möchten, sollten Sie zunächst das Paket insserv-compat installieren, um den Administrationsagenten konfigurieren.

8. Wenn Sie den Administrationsagenten auf Geräten installieren möchten, auf denen das Betriebssystem Astra Linux in der abgeschlossenen Softwareumgebung ausgeführt wird, führen Sie die zusätzlichen Schritte aus, um die Geräte mit Astra Linux vorzubereiten.

9. Wenn Sie den Administrationsagenten auf Geräten mit Ubuntu Server oder Ubuntu Desktop Version 10.04 installieren möchten, führen Sie die zusätzlichen Schritte aus, um diese Geräte vorzubereiten.

10. Wenn Sie den Administrationsagenten auf einem Gerät installieren möchten, auf dem ein Linux-Betriebssystem mit glibc 2.5 ausgeführt wird, führen Sie die zusätzlichen Schritte aus, um die Zielgeräte vorzubereiten.

11. Wenn Sie Administrationsagent auf AltOS im geschlossenen Softwareumgebungsmodus installieren, aktivieren Sie diesen Modus erneut.

12. Wenn Sie den Administrationsagenten auf Geräten mit den Betriebssystemen RED OS 7.3.4 und höher bzw. MSVSPHERE 9.2 und höher installieren möchten, installieren Sie das Paket "libxcrypt-compat", damit der Administrationsagent ordnungsgemäß funktioniert.

Das Linux-Gerät ist bereit für die Installation des Administrationsagenten. Sie können den Administrationsagenten remote, im interaktiven Modus oder im Silent-Modus installieren.

Ein Gerät mit SUSE Linux Enterprise Server 15 für die Installation des Administrationsagenten vorbereiten

Bevor Sie den Administrationsagenten auf einem Gerät mit SUSE Linux Enterprise Server 15 installieren können, müssen Sie zwei vorbereitende Maßnahmen ausführen: Zum einen die in der unteren Anleitung beschriebene und zum anderen die Schritte zur allgemeinen Vorbereitung eines beliebigen Linux-Geräts.

Um den Administrationsagenten auf einem Gerät mit dem Betriebssystem SUSE Linux Enterprise Server 15 zu installieren:

Führen Sie vor der Installation des Administrationsagenten den folgenden Befehl aus:

```
sudo zypper install insserv-compat
```

Dies erlaubt Ihnen die Installation des Pakets insserv-compat, um den Administrationsagenten richtig zu konfigurieren.

Führen Sie den Befehl `rpm -q insserv-compat` aus, um zu prüfen, ob das Paket bereits installiert ist.

Wenn Ihr Netzwerk viele Geräte mit SUSE Linux Enterprise Server 15 umfasst, können Sie das spezielle Programm zum Konfigurieren und Verwalten der Unternehmensinfrastruktur verwenden. Mittels dieses Programms können Sie das Paket insserv-compat automatisch auf allen erforderlichen Geräten gleichzeitig installieren. Sie können beispielsweise Puppet, Ansible, Chef oder Ihr selbsterstelltes Skript verwenden – je nachdem, was für Sie am besten geeignet ist.

Wenn das Gerät nicht über die GPG-Signaturschlüssel für SUSE Linux Enterprise verfügt, wird möglicherweise die folgende Warnung angezeigt: `Package header is not signed!` Um die Warnung zu ignorieren, wählen Sie die Option `i`.

Wenn Sie das Linux-Gerät vorbereitet haben, können Sie den Administrationsagenten remote, im interaktiven Modus oder im Silent-Modus installieren.

Ein Gerät auf dem Astra Linux im Modus der abgeschlossenen Softwareumgebung ausgeführt wird für die Installation des Administrationsagenten vorbereiten

Vor der Installation des Administrationsagenten auf einem Gerät mit Astra Linux in der abgeschlossenen Softwareumgebung müssen Sie zwei Schritte zur Vorbereitung ausführen: Zum einen den in der folgenden Anleitung beschriebenen und zum anderen den allgemeinen Schritt zur Vorbereitung eines beliebigen Linux-Geräts.

Führen Sie unter einem Benutzerkonto mit Root-Rechten die in dieser Anleitung genannten Befehle aus.

So bereiten Sie Gerät mit Astra Linux im Modus der abgeschlossenen Softwareumgebung für die Installation des Administrationsagenten vor:

1. Öffnen Sie die Datei `/etc/digsig/digsig_initramfs.conf` und geben Sie die folgende Einstellung an:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Führen Sie in der Befehlszeile den folgenden Befehl aus, um das Kompatibilitätspaket zu installieren:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Erstellen Sie ein Verzeichnis für den Anwendungsschlüssel:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Legen Sie den Anwendungsschlüssel /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gp in dem Verzeichnis ab, das Sie beim vorherigen Schritt erstellt haben:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Wenn der Anwendungsschlüssel "kaspersky_astra_pub_key.gpg" nicht im Lieferumfang von Kaspersky Security Center Linux enthalten ist, können Sie den Schlüssel über den folgenden Link herunterladen: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Aktualisieren Sie die RAM-Disks:

   ```
   update-initramfs -u -k all
   ```

   Starten Sie das System neu.

Das Linux-Gerät ist bereit für die Installation des Administrationsagenten. Sie können den Administrationsagenten remote, im interaktiven Modus oder im Silent-Modus installieren.

Installation des Administrationsagenten auf einem Linux-Betriebssystem mit glibc 2.5 (Legacy-Betriebssystem) vorbereiten

Bevor Sie den Administrationsagenten auf einem Gerät mit einem Linux-Betriebssystem mit glibc 2.5 (Legacy-Betriebssystem) installieren können, müssen Sie zwei vorbereitende Vorgänge ausführen: Zum einen die allgemeinen Schritte zur Vorbereitung eines beliebigen Linux-Geräts und zum anderen den in der folgenden Anleitung beschriebenen Vorgang.

Es wird empfohlen zur Installation des Administrationsagenten auf einem Linux-Betriebssystem mit glibc 2.5 (Legacy-Betriebssystem) die lokale Installation zu verwenden. Sollten Sie in diesem Szenario eine Remote-Installation benötigen, führen Sie zusätzlichen die unten beschriebenen Schritte aus.

> Führen Sie die in diesem Vorgang beschriebenen Befehle unter einem Benutzerkonto mit root-Berechtigung aus.

Es wird empfohlen zur Installation des Administrationsagenten auf einem Linux-Betriebssystem mit glibc 2.5 (Legacy-Betriebssystem) die lokale Installation zu verwenden. Sollten Sie in diesem Szenario eine Remote-Installation benötigen, führen Sie zusätzlichen die unten beschriebenen Schritte aus.

1. Führen Sie auf einem Gerät mit Linux-Betriebssystem und glibc 2.5 die vorbereitenden Schritte aus, die für jedes beliebige Linux-Gerät gelten.

2. Entfernen Sie in der Datei `/etc/sudoers` die Zeile `Defaults requiretty`.

3. Deaktivieren Sie die Allow-Liste der zulässigen Verschlüsselungsalgorithmen für SSH-Verbindungen, um den Administrationsagenten auf dem Gerät mit Linux-Betriebssystem und glibc 2.5 installieren zu können.

   Führen Sie dazu auf dem Gerät mit dem installierten Administrationsserver oder auf einem Gerät, das als Verteilungspunkt fungiert und dessen Gültigkeitsbereich das Zielgerät umfasst, den folgenden Befehl in der Befehlszeile aus:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

Das Linux-Gerät ist bereit für die Remote-Installation des Administrationsagenten.

Das Deaktivieren der Allow-Liste mit gültigen Verschlüsselungsalgorithmen kann die Sicherheit der SSH-Verbindung beeinträchtigen. Es wird dringend empfohlen, die Allow-Liste mit gültigen Verschlüsselungsalgorithmen sofort nach der Installation des Administrationsagenten wieder zu aktivieren. Um die Allow-Liste mit zulässigen Verschlüsselungsalgorithmen wieder zu aktivieren, führen Sie folgenden Befehl aus:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

Wenn Sie den Administrationsagenten installiert und die Allow-Liste der zulässigen Verschlüsselungsalgorithmen wieder aktiviert haben, wird das Gerät mit Linux-Betriebssystem mit glibc 2.5 (Legacy-Betriebssystem) durch den Administrationsserver verwaltet.

Installation des Administrationsagenten auf einem Linux-Betriebssystem mit OpenSSH-Version 6.4 (Legacy-Betriebssystem) vorbereiten

Bevor Sie den Administrationsagenten auf einem Gerät installieren können, das die OpenSSH-Version 6.4 oder niedriger (Legacy-Betriebssystem) verwendet, müssen Sie zwei vorbereitende Maßnahmen durchführen: die allgemeinen Schritte zur Vorbereitung eines beliebigen Linux-Geräts und das in diesem Artikel beschriebene Verfahren.

Es wird empfohlen zur Installation des Administrationsagenten auf einem Linux-Betriebssystem mit glibc 2.5 (Legacy-Betriebssystem) die lokale Installation zu verwenden. Sollten Sie in diesem Szenario eine Remote-Installation benötigen, führen Sie zusätzlichen die unten beschriebenen Schritte aus.

> Führen Sie unter einem Benutzerkonto mit Root-Rechten die in dieser Anleitung genannten Befehle aus.

So bereiten Sie ein Gerät, das OpenSSH in Version 6.4 oder früher verwendet, für die Installation des Administrationsagenten vor:

1. Führen Sie auf dem Gerät, das OpenSSH in Version 6.4 oder früher verwendet, die vorbereitenden Schritte aus, die für alle Linux-Geräte gleich sind.

2. Deaktivieren Sie die Allow-Liste der zulässigen Verschlüsselungsalgorithmen für SSH-Verbindungen, um den Administrationsagenten auf einem Gerät zu installieren, welches die OpenSSH-Version 6.4 oder niedriger verwendet.

   Führen Sie dazu auf dem Gerät mit dem installierten Administrationsserver oder auf einem Gerät, das als Verteilungspunkt fungiert und dessen Gültigkeitsbereich das Zielgerät umfasst, den folgenden Befehl in der Befehlszeile aus:

   ```
   klscflag -fset -pv ".core/.independent" -s "Transport" -n
   SSH_CLIENT_DISABLE_ALGS_PROTECT -t d -v 1
   ```

Das Linux-Gerät ist bereit für die Remote-Installation des Administrationsagenten.

Das Deaktivieren der Allow-Liste mit gültigen Verschlüsselungsalgorithmen kann die Sicherheit der SSH-Verbindung beeinträchtigen. Es wird dringend empfohlen, die Allow-Liste mit gültigen Verschlüsselungsalgorithmen sofort nach der Installation des Administrationsagenten wieder zu aktivieren. Um die Allow-Liste mit zulässigen Verschlüsselungsalgorithmen wieder zu aktivieren, führen Sie folgenden Befehl aus:

```
klscflag -fset -pv ".core/.independent" -s "Transport" -n SSH_CLIENT_DISABLE_ALGS_PROTECT
-t d -v 0
```

Wenn Sie den Administrationsagenten installiert und die Allow-Liste der zulässigen Verschlüsselungsalgorithmen wieder aktiviert haben, wird das Gerät mit Linux-Betriebssystem mit glibc 2.5 (Legacy-Betriebssystem) durch den Administrationsserver verwaltet.

Administrationsagent auf einem Linux-Gerät remote installieren

Bevor Sie den Administrationsagenten auf einem Linux-basierten Gerät installieren können, müssen Sie die allgemeinen vorbereitende Schritte abschließen, die für jedes Linux Gerät erforderlich sind.

Wenn Sie die allgemeinen Schritte abgeschlossen haben, können Sie die zusätzlichen Anweisungen für Ihr Betriebssystem befolgen:

- Ein Gerät mit SUSE Linux Enterprise Server 15 vorbereiten
- Ein Gerät mit Astra Linux im Modus der abgeschlossenen Softwareumgebung vorbereiten
- Ein Gerät mit Ubuntu Server/Desktop Version 10.04 und 16.04 vorbereiten
- Ein Gerät mit einem Linux-Betriebssystem mit glibc 2.5 vorbereiten

So installieren Sie den Administrationsagenten remote auf Linux-Geräten:

1. Laden Sie das Installationspaket herunter und erstellen Sie es:

   a. Vergewissern Sie sich vor der Installation des Pakets, dass die Abhängigkeiten für das jeweilige Paket (Programme, Bibliotheken) auf dem Gerät installiert sind.

   Sie können die Abhängigkeiten für jedes Paket selbständig anzeigen, indem Sie die Tools verwenden, die für den Linux- Distributionssatz spezifiziert sind, auf dem das Paket installiert wird. Mit den Informationen über die Tools können Sie sich in der Dokumentation zu Ihrem Betriebssystem vertraut machen.

   b. Verwenden Sie folgende Dateien, um ein Installationspaket für Remote-Installation zu erstellen:

   - klnagent.kpd.
   - akinstall.sh.
   - deb- oder rpm-Paket des Administrationsagenten.

2. Erstellen Sie eine Aufgabe zur Remote-Installation des Programms mit den folgenden Einstellungen:

   - Aktivieren Sie auf der Seite **Einstellungen** des Assistenten für das Erstellen einer Aufgabe das Kontrollkästchen **Durch Ressourcen des Betriebssystems über den Administrationsserver**. Deaktivieren Sie alle anderen Kontrollkästchen.
   - Geben Sie auf der Seite **Benutzerkonto für die Ausführung der Aufgabe auswählen** die Einstellungen des Benutzerkontos an, das für die SSH-Verbindung mit dem Gerät verwendet wird.

3. Starten Sie die Aufgabe zur Remote-Installation des Programms. Verwenden Sie die Option für den Befehl `su`, um die Umgebung beizubehalten: `-m, -p, --preserve-environment`.

Administrationsagent für Linux im Silent-Modus installieren (mit einer Antwort-Datei)

Auf Linux können Sie den Administrationsagenten installieren, indem Sie eine Antwort-Datei verwenden. Dabei handelt es sich im eine Textdatei mit benutzerdefinierten Menge an Installationsparametern: Variablen und ihre entsprechenden Werte. Unter Verwendung der Antwort-Datei können Sie die Installation im Silent-Modus, d. h. ohne Benutzerbeteiligung, ausführen.

Bevor Sie den Administrationsagenten auf einem Linux-basierten Gerät installieren können, müssen Sie die allgemeinen vorbereitende Schritte abschließen, die für jedes Linux Gerät erforderlich sind.

Wenn Sie die allgemeinen Schritte abgeschlossen haben, können Sie die zusätzlichen Anweisungen für Ihr Betriebssystem befolgen:

- Ein Gerät mit SUSE Linux Enterprise Server 15 vorbereiten
- Ein Gerät mit Astra Linux im Modus der abgeschlossenen Softwareumgebung vorbereiten
- Ein Gerät mit Ubuntu Server/Desktop Version 10.04 und 16.04 vorbereiten
- Ein Gerät mit einem Linux-Betriebssystem mit glibc 2.5 vorbereiten

Um den Administrationsagent für Linux im Silent-Modus zu installieren:

1. Lesen Sie den Endbenutzer-Lizenzvertrag. Folgen Sie den unten aufgeführten Schritten nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.
2. Erstellen Sie die Antwortdatei (im txt-Format). Fügen Sie der Datei eine Liste mit Variablen im Format "NAME_DER_VARIABLEN=wert_der_variablen" hinzu. Dabei muss jede Variable in einer separaten Zeile angegeben werden.

   Damit die Antwort-Datei korrekt funktioniert, müssen Sie in ihr mindestens diese drei notwendigen Variablen angeben:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Sie können auch weitere Variablen hinzufügen, um spezifischere Parameter für Ihre Remote-Installation zu verwenden. Die folgende Tabelle enthält eine Liste aller Variablen, die in der Antwort-Datei enthalten sein können:

   Für die Installation des Administrationsagenten für Linux im Silent-Modus genutzte Parameter der Antwort-Datei

   Für die Installation des Administrationsagenten für Linux im Silent-Modus genutzte Parameter der Antwort-Datei

Name der Variablen	Erforderlich	Beschreibung	Mögliche Werte
KLNAGENT_SERVER	Ja	Beinhaltet den Name des Administrationsservers in Form des voll qualifizierten Domänennamens (FQDN) oder der IP-Adresse.	DNS-Name oder IP-Adresse.
KLNAGENT_AUTOINSTALL	Ja	Gibt an, ob der Silent-Modus für die Installation aktiviert ist.	1—Der Silent-Modus ist aktiviert und der Benutzer erhält während der Installation keinerlei Aufforderungen, etwas zu tun. Andere—Der Silent-Modus ist deaktiviert und der Benutzer kann während der Installation Aufforderungen erhalten, etwas zu tun.

EULA_ACCEPTED	Ja	Gibt an, ob der Benutzer den Endbenutzer-Lizenzvertrag (EULA) des Administrationsagenten akzeptiert hat. Ein Fehlen des Parameters wird als Ablehnung der EULA interpretiert.	1 – Ich bestätige, dass ich die Bestimmungen und Bedingungen dieses Endbenutzer-Lizenzvertrags vollständig gelesen habe und sie verstehe und akzeptiere. Anderer Wert oder keine Angabe – Ich akzeptiere die Bedingungen des Endbenutzer-Lizenzvertrags nicht (die Installation wird nicht ausgeführt).
KLNAGENT_PROXY_USE	Nein	Gibt an, ob die Verbindung zum Administrationsserver Proxy-Einstellungen verwendet. Als Standardwert ist 0 vorgegeben.	1—Die Proxy-Einstellungen werden verwendet. Andere—Die Proxy-Einstellungen werden nicht verwendet.
KLNAGENT_PROXY_ADDR	Nein	Gibt die Adresse des Proxyservers an, der für die Verbindung mit dem Administrationsserver verwendet wird.	DNS-Name oder IP-Adresse.
KLNAGENT_PROXY_LOGIN	Nein	Gibt den Benutzernamen an, der für die Anmeldung am Proxyserver verwendet wird.	Ein beliebiger existierender Benutzername.
KLNAGENT_PROXY_PASSWORD	Nein	Gibt Kennwort des Benutzers an, das für die Anmeldung am Proxyserver verwendet wird.	Ein beliebiger Satz aus alphanumerischen Zeichen, die für das Kennwort-Format des Betriebssystems zulässig sind.
KLNAGENT_VM_VDI	Nein	Gibt an, ob der Administrationsagent auf einem Abbild zur Erstellung dynamischer virtueller Maschinen installiert wird.	1—Der Administrationsagent wird auf einem Abbild installiert, welches anschließend für die Erstellung dynamischer virtueller Maschinen genutzt wird. Andere—Während der Installation wird kein Abbild verwendet.
KLNAGENT_VM_OPTIMIZE	Nein	Gibt an, ob die Administrationsagent-Einstellungen optimal für Hypervisor sind.	1—Die standardmäßigen lokalen Administrationsagent-Einstellungen wurden angepasst, so dass sie eine optimale Verwendung auf Hypervisor erlauben.
KLNAGENT_TAGS	Nein	Liste der Tags, die der Instanz des Administrationsagenten zugewiesen wurden.	Ein oder mehrere Tag-Namen, getrennt durch ein Semikolon.
KLNAGENT_UDP_PORT	Nein	Gibt den vom Administrationsagenten verwendeten UDP-Port an. Als Standardwert ist 15000 vorgegeben.	Eine beliebige existierende Portnummer.
KLNAGENT_PORT	Nein	Gibt den vom Administrationsagenten verwendeten Non-TLS-Port an. Als Standardwert ist 14000 vorgegeben.	Eine beliebige existierende Portnummer.
KLNAGENT_SSLPORT	Nein	Gibt den vom Administrationsagenten verwendeten TLS-Port an. Als Standardwert ist 13000 vorgegeben.	Eine beliebige existierende Portnummer.

KLNAGENT_USESSL	Nein	Gibt an, ob Transport Layer Security (TLS) für die Verbindung verwendet wird.	1 (Standard)—TLS wird verwendet. Andere—TLS wird nicht verwendet.
KLNAGENT_GW_MODE	Nein	Gibt an, ob ein Verbindungsgateway verwendet wird.	1 (Standard)—Die aktuellen Einstellungen wurden nicht geändert (Beim ersten Aufruf ist kein Verbindungsgateway angegeben). 2—Es wird kein Gateway verwendet. 3—Es wird ein Gateway verwendet. KLNAGENT_GW_ADDRESS ist erforderlich. 4—Die Instanz des Administrationsagenten wird als Verbindungsgateway in die demilitarisierte Zone (DMZ) verwendet. Serverzertifikat ist erforderlich.
KLNAGENT_GW_ADDRESS	Nein	Gibt die Adresse des Verbindungsgateways an. Der Wert wird nur ausgewertet, wenn "KLNAGENT_GW_MODE=3" gesetzt ist.	DNS-Name oder IP-Adresse.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Nein	Ermöglicht nach der Installation des Administrationsagenten die Ausführung des Tools zum Registrieren von Benutzern als Gerätebesitzer. Bei deaktivierter Option, steht dem Benutzer die Registrierung als Gerätebesitzer nicht zur Verfügung.	1—Das Tools zum Registrieren von Benutzern als Gerätebesitzer wird nach der Installation des Administrationsagenten ausgeführt. Andere—Deaktiviert.
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	Nein	Legt fest, ob heruntergeladene Updates für den Administrationsagenten mit dem Status *Nicht definiert* automatisch installiert werden sollen.	true (Standardwert) – Updates werden automatisch installiert. false – Updates werden nicht automatisch installiert.

3. Installieren Sie den Administrationsagenten. Die Umgebungsvariable KLAUTOANSWERS, in welcher der Pfad zur Antwort-Datei angegeben ist, wird an den Installationsbefehl übergeben. Führen Sie einen der folgenden Befehle aus:

   - Um den Administrationsagenten aus einem RPM-Paket auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
     `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> yum install ./klnagent-<Build-Nummer>.i386.rpm`

   - Um den Administrationsagenten aus einem RPM-Paket auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
     `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> yum install ./klnagent64-<Build-Nummer>.x86_64.rpm`

   - Um den Administrationsagenten aus einem RPM-Paket auf einem 64-Bit-Betriebssystem für die ARM-Architektur zu installieren, führen Sie den folgenden Befehl aus:
     `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> yum install ./klnagent64-<Build-Nummer>.aarch64.rpm`

- Um den Administrationsagenten aus einem DEB-Paket auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
  `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> apt install ./klnagent_<Build-Nummer>_i386.deb`

- Um den Administrationsagenten aus einem DEB-Paket auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
  `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> apt install ./klnagent64_<Build-Nummer>_amd64.deb`

- Um den Administrationsagenten von einem DEB-Paket auf einem 64-Bit-Betriebssystem für die ARM-Architektur zu installieren, führen Sie den folgenden Befehl aus:
  `sudo KLAUTOANSWERS=<Pfad zur Antwortdatei> apt install ./klnagent64_<Build-Nummer>_arm64.deb`

Je nach Konfiguration des Betriebssystems können Sie zur Installation des Administrationsagenten auch die Paketmanager rpm, dpkg oder dnf verwenden.

Die Installation des Administrationsagenten für Linux wird im Silent-Modus gestartet und der Benutzer erhält während des Vorgangs keinerlei Aufforderungen, etwas zu tun.

Administrationsagent für Linux im interaktiven Modus installieren

Dieser Artikel beschreibt, wie Sie den Administrationsagenten auf Linux-Geräten im interaktiven Modus installieren. In diesem Modus können Sie die Installationsparameter Schritt für Schritt angeben. Alternativ dazu können Sie eine Antwortdatei verwenden. Dies ist eine Textdatei mit benutzerdefinierten Installationsparametern: Variablen und deren Werte. Unter Verwendung dieser Antwortdatei können Sie die Installation im Silent-Modus ausführen, d. h. ohne Benutzerbeteiligung.

Bevor Sie den Administrationsagenten auf einem Linux-basierten Gerät installieren können, müssen Sie die allgemeinen vorbereitende Schritte abschließen, die für jedes Linux Gerät erforderlich sind.

Wenn Sie die allgemeinen Schritte abgeschlossen haben, können Sie die zusätzlichen Anweisungen für Ihr Betriebssystem befolgen:

- Ein Gerät mit SUSE Linux Enterprise Server 15 vorbereiten
- Ein Gerät mit Astra Linux im Modus der abgeschlossenen Softwareumgebung vorbereiten
- Ein Gerät mit Ubuntu Server/Desktop Version 10.04 und 16.04 vorbereiten
- Ein Gerät mit einem Linux-Betriebssystem mit glibc 2.5 vorbereiten

So installieren Sie den Administrationsagenten im interaktiven Modus:

1. Installieren Sie den Administrationsagenten. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:

   - So installieren Sie den Administrationsagenten aus einem RPM-Paket auf einem 32-Bit-Betriebssystem:
     `# yum -i klnagent-<Build-Nummer>.i386.rpm`

   - So installieren Sie den Administrationsagenten aus einem RPM-Paket auf einem 64-Bit-Betriebssystem:
     `# yum -i klnagent64-<Build-Nummer>.x86_64.rpm`

- So installieren Sie den Administrationsagenten aus einem RPM-Paket auf einem 64-Bit-Betriebssystem für die Arm-Architektur:

  ```
  # yum -i klnagent64-<Build-Nummer>.aarch64.rpm
  ```

- So installieren Sie den Administrationsagenten aus einem DEB-Paket auf einem 32-Bit-Betriebssystem:

  ```
  # apt install ./klnagent_<Build-Nummer>_i386.deb
  ```

- So installieren Sie den Administrationsagenten aus einem DEB-Paket auf einem 64-Bit-Betriebssystem:

  ```
  # apt install ./klnagent64_<Build-Nummer>_amd64.deb
  ```

- So installieren Sie den Administrationsagenten aus einem DEB-Paket auf einem 64-Bit-Betriebssystem für die Arm-Architektur:

  ```
  # apt install ./klnagent64_<Build-Nummer>_arm64.deb
  ```

2. Konfigurieren Sie den Administrationsagenten:

   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Lesen Sie den Endbenutzer-Lizenzvertrag (EULA). Der Text wird im Befehlszeilenfenster angezeigt. Drücken Sie die Leertaste, um das nächste Textsegment anzuzeigen. Geben Sie nach der entsprechenden Aufforderung einen der folgenden Werte ein:

   - Geben Sie `y` ein, wenn Sie die EULA-Bedingungen verstehen und akzeptieren.
   - Geben Sie `n` ein, wenn Sie den EULA-Bedingungen nicht zustimmen. Um den Administrationsagenten zu nutzen, müssen Sie den EULA-Bestimmungen zustimmen.
   - Geben Sie `r` ein, um die EULA erneut anzuzeigen.

4. Geben Sie den DNS-Namen oder die IP-Adresse des Administrationsservers ein.

5. Geben Sie die Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 14000 festgelegt.

6. Geben Sie die SSL-Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 13000 festgelegt.

7. Geben Sie `y` ein, wenn Sie für den Datenverkehr zwischen dem Administrationsagenten und dem Administrationsserver die SSL-Verschlüsselung verwenden möchten. Andernfalls geben Sie `n` ein.

8. Wählen Sie eine der folgenden Methoden für die Konfiguration des Administrationsagenten aus:

   - `[1]` – Verbindungs-Gateway nicht konfigurieren.

     Ihr Gerät fungiert nicht als Verbindungs-Gateway und stellt keine Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway her.

   - `[2]` – Verbindungs-Gateway nicht verwenden.

     Ihr Gerät stellt keine Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway her.

   - `[3]` – Verbindungs-Gateway für die Verbindung mit dem Server verwenden.

     Ihr Gerät stellt eine Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway her.

- [4] – Als Verbindungs-Gateway verwenden.

  Ihr Gerät fungiert als Verbindungs-Gateway.

Der Administrationsagent wird auf einem Linux-Gerät installiert.

Unterstützung des Rollbacks des Dateisystems für Geräte mit Administrationsagent

Kaspersky Security Center Linux ist ein verteiltes Programm. Ein Rollback des Dateisystems auf den vorhergehenden Zustand auf einem der Geräte mit installiertem Administrationsagenten führt zu einer Desynchronisierung der Daten und zur fehlerhaften Ausführung von Kaspersky Security Center Linux.

Ein Rollback des Dateisystems (oder eines Teils davon) auf den vorhergehenden Zustand kann in folgenden Fälle durchgeführt werden:

- Beim Kopieren eines Festplatten-Image.
- Bei der Wiederherstellung des Status der virtuellen Maschine mithilfe der virtuellen Infrastruktur.
- Beim Wiederherstellen der Daten aus der Backup-Kopie oder einem Wiederherstellungspunkt.

Szenarien, in denen Drittanbieter-Programme auf Geräten mit installiertem Administrationsagenten das Verzeichnis "/var/opt/kaspersky/klnagent" betreffen, stellen nur für Kaspersky Security Center Linux kritische Szenarien dar. Deshalb ist es erforderlich, diesen Ordner, wenn möglich immer aus der Wiederherstellungsprozedur auszuschließen.

Da in einer Reihe von Unternehmen die Dienstordnung das Ausführen eines Rollbacks des Zustandes des Dateisystems der Geräte voraussetzt, wurde in Kaspersky Security Center Linux ab Version 10 Maintenance Release 1 (Administrationsserver und die Administrationsagenten müssen Versionen 10 Maintenance Release 1 oder höher sein) die Unterstützung der Erkennung eines Rollbacks des Dateisystems auf den Geräten mit installiertem Administrationsagenten hinzugefügt. Im Fall des Erkennens werden solche Geräte automatisch mit einem Administrationsserver mit vollständiger Bereinigung und vollständiger Synchronisierung der Daten verbunden.

In Kaspersky Security Center Linux ist die Unterstützung des Erkennens eines Rollbacks des Dateisystems standardmäßig aktiviert.

Es wird dringend empfohlen, ein Rollback des Verzeichnisses "/var/opt/kaspersky/klnagent" auf Geräten mit installiertem Administrationsagenten zu vermeiden, da eine erneute vollständige Synchronisierung der Daten einen großen Teil der Ressourcen fordert.

Für das Gerät mit installiertem Administrationsserver ist ein Rollback des Systemzustands unzulässig. Ebenfalls unzulässig ist ein Rollback auf den vorhergehenden Zustand der Datenbank, die vom Administrationsserver verwendet wird.

Der Zustand des Administrationsservers kann nur mithilfe des Standardtools klbackup aus der Backup-Kopie wiederhergestellt werden.

Administrationsagent für Windows installieren

Sie können den Administrationsagenten auch auf den Windows-Geräten einer Organisation installieren, um sie anschließend über den Administrationsserver zu verwalten.

Unter Windows XP führt der Administrationsagent folgende Operationen möglicherweise nicht korrekt aus: Das Herunterladen von Updates direkt von den Servern von Kaspersky (als Verteilungspunkt), das Fungieren als KSN-Proxyserver (als Verteilungspunkt) und das Erkennen von Schwachstellen bei Drittanbietern (wenn die Funktion Schwachstellen- und Patch-Management genutzt wird).

Bevor Sie den Administrationsagenten auf einem Gerät mit Microsoft Windows on ARM installieren, stellen Sie sicher, dass nicht bereits ein Administrationsagent für Microsoft Windows x86-64 installiert ist. Andernfalls schlägt die Installation fehl.

Die folgenden Methoden stehen zur erstmaligen Installation des Administrationsagenten auf einem verwalteten Windows-Gerät zur Verfügung:

- Durch Ausführen der Aufgabe zur Remote-Installation über einen Windows-basierten Verteilungspunkt.

  Bevor die Remote-Installation auf einem nicht zugeordneten Windows-Gerät ausgeführt wird, überprüft ein Windows-basierter Verteilungspunkt automatisch den UDP-Port 137, um das Betriebssystem des Zielgeräts zu bestimmen. Wenn der UDP-Port 137 nicht verfügbar ist, versucht der Verteilungspunkt, auf dem Zielgerät eine Verbindung mit dem für die Installation erforderlichen TCP-Port 445 herzustellen.

- Durch Verwenden des Windows Installer-Paket (msi-Datei) für den Administrationsagenten und Drittanbieter-Tools zur Remote-Installation von Anwendungen.

- Durch Ausführen des Anwendungs-Installers auf dem verwalteten Gerät.

- Indem Sie den Gerätebenutzern Links zu den autonomen Paketen schicken, die von Kaspersky Security Center Linux erstellt wurden. Autonomen Pakete sind ausführbare Module, in denen die Programmpakete der ausgewählten Programme mit den konfigurierten Einstellungen enthalten sind.

Administrationsagent für Windows im interaktiven Modus installieren

Um den Administrationsagenten lokal auf einem Gerät zu installieren, gehen Sie wie folgt vor:

1. Starten Sie auf dem Gerät die Datei "ksc_<Versionsnummer>.<Build-Nummer>_full_<Sprache>.exe" des Programmpakets, dass Sie aus dem Internet heruntergeladen haben.

   Ein Fenster wird geöffnet, in dem Sie Kaspersky-Anwendungen zur Installation auswählen können.

2. Starten Sie im Fenster mit der Programmauswahl über den Link **Nur den Kaspersky Security Center Administrationsagenten installieren** den Installationsassistenten des Administrationsagenten. Folgen Sie den Anweisungen des Assistenten.

   Bei der Ausführung des Installationsassistenten können Sie die erweiterten Einstellungen des Administrationsagenten anpassen (s. unten).

3. Soll ein Gerät als Verbindungs-Gateway für eine gewählte Administrationsgruppe verwendet werden, wählen Sie im Fenster **Verbindungs-Gateway** des Installationsassistenten die Option **Administrationsagent als Verbindungs-Gateway in der DMZ verwenden**.

4. Um den Administrationsagenten bei der Installation auf der virtuellen Maschine anzupassen, gehen Sie wie folgt vor:

   a. Wenn Sie vorhaben, dynamische virtuelle Maschinen vom Image der virtuellen Maschine zu erstellen, aktivieren Sie den dynamischen Modus des Administrationsagenten für Virtual Desktop Infrastructure (VDI). Aktivieren Sie dazu im Fenster **Erweiterte Einstellungen** des Installationsassistenten die Option **Dynamischen Modus für VDI aktivieren**.

      Sie können diesen Schritt überspringen, wenn Sie nicht vorhaben, dynamische virtuelle Maschinen aus dem Image der virtuellen Maschinen zu erstellen.

   b. Optimieren Sie die Arbeit des Administrationsagenten für VDI. Aktivieren Sie dazu im Fenster **Erweiterte Einstellungen** des Installationsassistenten die Option **Einstellungen für VM optimieren**.

      Daraufhin wird die Prüfung der ausführbaren Dateien auf Schwachstellen beim Start des Geräts deaktiviert. Außerdem wird die Übertragung folgender Informationen auf den Administrationsserver deaktiviert:

      - Hardware-Register
      - Auf dem Gerät installierten Programme
      - Microsoft Windows-Updates, die auf dem lokalen Client-Gerät installiert werden sollen
      - Auf dem lokalen Client-Gerät gefundene Schwachstellen in Programmen

      Im Folgenden können Sie die Übertragung dieser Informationen in den Eigenschaften des Administrationsagenten oder in den Einstellungen der Richtlinie des Administrationsagenten aktivieren.

Nach Abschluss des Installationsassistenten wird der Administrationsagent auf dem Gerät installiert.

Sie können sich die Eigenschaften für den Dienst des Administrationsagenten anzeigen lassen, den Administrationsagenten starten und beenden sowie seine Ausführung mit den Standard-Administrationswerkzeugen von Microsoft Windows (Computerverwaltung\Dienste) verfolgen.

Administrationsagent für Windows im Silent-Modus installieren

Der Administrationsagent kann im Silent-Modus installiert werden, d. h. ohne die interaktive Eingabe von Installationsparametern. Bei der Installation im Silent-Modus wird ein Windows Installer-Paket (msi-Datei) für den Administrationsagenten verwendet. Die msi-Datei befindet sich im Programmpaket für Kaspersky Security Center Linux im Ordner Packages\NetAgent\exec.

> Die Installation des Administrationsagenten mittels msi-Paket ist nur im Silent-Modus möglich. Die interaktive Installation mittels msi-Paket wird nicht unterstützt.

Um den Administrationsagenten im Silent-Modus auf einem lokalen Gerät zu installieren:

1. Lesen Sie den Endbenutzer-Lizenzvertrag. Verwenden Sie den unten angegebenen Befehl nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.

2. geben Sie folgenden Befehl ein:

```
msiexec /i "Kaspersky Network Agent.msi" /qn <Parameters>
```

Dabei steht `Parameter` für eine Liste mit Einstellungen und deren Werten, die durch Leerzeichen getrennt werden (`PROP1=PROP1VAL PROP2=PROP2VAL`).

In der Liste der Parameter müssen Sie `EULA=1` aufnehmen. Andernfalls wird der Administrationsagent nicht installiert.

Wenn Sie die standardmäßigen Verbindungseinstellungen für Kaspersky Security Center und den Administrationsagenten auf Remote-Geräten verwenden, führen Sie den folgenden Befehl aus:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` ist der Schlüssel für das Erstellen von Protokollen. Das Protokoll wird im Zuge des Administrationsagenten erstellt und abgespeichert unter C:\windows\temp\nag_inst.log.

Zusätzlich zum Protokoll "ag_inst.log" erstellt das Programm die Datei "$klssinstlib.log", welche das Installationsprotokoll enthält. Die Datei wird in den folgenden Ordnern gespeichert: %windir%\temp oder %temp%. Für etwaige Fehlerbehebungen kann es möglich sein, dass Sie oder ein Spezialist des Technischen Supports von Kaspersky beide Protokolldateien benötigen: "nag_inst.log" und "$klssinstlib.log".

Wenn Sie zusätzlich den Port für die Verbindung zu einem Administrationsserver angeben möchten, führen Sie den folgenden Befehl aus:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

Der Parameter `SERVERPORT` entspricht der Portnummer für die Verbindung zum Administrationsserver.

Die Namen und die möglichen Werte für Einstellungen, die bei der Installation des Administrationsagenten im Silent-Modus verwendet werden können, sind im Abschnitt Installationseinstellungen für den Administrationsagenten angegeben.

Wenn Sie den Administrationsagenten mithilfe von Windows Installer aktualisieren möchten, führen Sie den folgenden Befehl aus:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Bereitstellung durch Erstellung und Verteilung eines Geräte-Images

Wenn der Administrationsagent auf den Geräten installiert werden muss, auf denen auch das Betriebssystem und die übrige Software installiert (bzw. neu installiert) werden sollen, ist es möglich, den Mechanismus zum Erstellen und Kopieren eines Geräte-Images zu verwenden.

Um die Bereitstellung durch das Erstellen und Kopieren einer Festplatte auszuführen:

1. Erstellen Sie ein Referenzgerät mit einem Betriebssystem und installieren Sie darauf die erforderliche Software, einschließlich Administrationsagent und Sicherheitsanwendung.

2. Erstellen Sie ein Image des Mustergeräts und verteilen Sie dieses Image anschließend mit der dafür vorgesehenen Aufgabe von Kaspersky Security Center Linux auf die neuen Geräte.

   Verwenden Sie zum Erstellen und Installieren von Festplatten-Images Tools von Drittanbietern, die im Unternehmen verfügbar sind.

Kopieren des Festplatten-Images mittels Drittanbieter-Tools

Bei Verwendung von Tools von Drittherstellern für das Aufzeichnen des Images des Geräts mit dem installierten Administrationsagenten muss eine der folgenden Methoden verwendet werden:

- Beenden Sie auf dem Referenzgerät den Dienst des Administrationsagenten und führen Sie das Tool "klmover" mit dem Parameter `-dupfix` aus. Das Tool klmover ist Teil des Installationspakets des Administrationsagenten. Vermeiden Sie die erneute Ausführung des Administrationsagenten, bis der Vorgang zum Aufzeichnen des Images abgeschlossen ist.

- Stellen Sie sicher, dass das Tool "klmover" vor dem ersten Start des Dienstes des Administrationsagenten auf den Zielgeräten mit dem Schlüssel `-dupfix` ausgeführt wird. Dies ist eine zwingende Voraussetzung und muss beim ersten Start des Betriebssystems nach der Bereitstellung des Images durchgeführt werden. Das Tool "klmover" ist Teil des Installationspakets des Administrationsagenten.

- Verwenden Sie den "Laufwerk klonen"-Modus des Administrationsagenten.

Wenn das Festplatten-Image fehlerhaft kopiert wurde, können Sie das Problem beheben.

Sie können auch ein Image von einem Gerät erstellen, auf dem der Administrationsagent nicht installiert ist. Verteilen Sie dazu die Images auf den Zielgeräten und stellen Sie anschließend den Administrationsagenten bereit. Wenn Sie diese Methode verwenden, müssen Sie den Zugriff auf den Netzwerkordner mit autonomen Installationspaketen von einem Gerät aus gewähren.

Modus des Administrationsagenten zum Klonen von Laufwerken

Das Klonen der Festplatte eines Referenzgerätes ist eine verbreitete Methode zur Installation von Software auf neuen Geräten. Wenn der Administrationsagent auf der Festplatte des Referenzgerätes während des Klonens im Standardmodus ausgeführt wird, kann das folgende Problem auftreten:

Nach der Bereitstellung des Referenz-Images der Festplatte mit dem Administrationsagenten auf den neuen Geräten werden diese Geräte in der Kaspersky Security Center Web Console als ein einziges Gerät dargestellt. Das Problem tritt auf, weil beim Klonen auf den neuen Geräten identische interne Daten beibehalten werden, die es dem Administrationsserver erlauben, das Gerät mit dessen eigenen Eintrag in der Kaspersky Security Center Web Console zu verknüpfen.

Die Probleme mit der inkorrekten Anzeige neuer Geräte in der Kaspersky Security Center Web Console nach dem Klonen können mithilfe des speziellen *Laufwerk klonen-Modus des Administrationsagenten* vermieden werden. Verwenden Sie diesen Modus, wenn Sie die Software (mit dem Administrationsagenten) auf neuen Geräten mittels der Laufwerk klonen-Methode verteilen.

Im Laufwerk klonen-Modus wird der Administrationsagent ausgeführt, stellt aber keine Verbindung mit Administrationsserver her. Beim Ausschalten des Laufwerk klonen-Modus löscht der Administrationsagent die internen Daten, aufgrund deren der Administrationsserver mehrere Geräte mit einem Eintrag in der Kaspersky Security Center Web Console verknüpft. Nach Abschluss des Klonens des Referenzgerät-Images werden neue Geräte in der Kaspersky Security Center Web Console korrekt (als separate Geräte) angezeigt.

Handlungsempfehlung für den "Laufwerk klonen"-Modus des Administrationsagenten

1. Der Administrator installiert den Administrationsagenten auf dem Client-Gerät.
2. Der Administrator überprüft die Verbindung des Administrationsagenten mit dem Administrationsserver mithilfe des Tools "klnagchk".
3. Der Administrator aktiviert den "Laufwerk klonen"-Modus des Administrationsagenten.
4. Der Administrator installiert Software und Patches auf dem Gerät und führt eine beliebige Anzahl von Geräteneustarts aus.
5. Der Administrator nimmt das Klonen des Referenzgerät-Laufwerks auf beliebig vielen Geräten vor.
6. Für jede geklonte Kopie müssen folgende Bedingungen erfüllt sein:
   a. Der Geräte wurde geändert
   b. Das Gerät wurde Neu starten
   c. Der "Laufwerk klonen"-Modus wurde deaktiviert

Den "Laufwerk klonen"-Modus mithilfe des Tools "klmover" aktivieren und deaktivieren

Um den "Laufwerk klonen"-Modus des Administrationsagenten zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Starten Sie das Tool klmover auf dem Gerät mit dem installierten Administrationsagenten, das geklont werden soll.

   Das klmover-Dienstprogramm befindet sich im Installationsordner des Administrationsagenten.

2. Um den „Laufwerk klonen“-Modus zu aktivieren, geben Sie in der Linux-Kommandozeile den Befehl:

   ```
   ./klmover -cloningmode 1
   ```

   Der Administrationsagent schaltet in den Modus zum Klonen von Laufwerken.

3. Um den aktuellen Status des den Modus zum Klonen von Laufwerken abzurufen, geben Sie in der Kommandozeile den folgenden Befehl ein:

   ```
   ./klmover -cloningmode
   ```

   Im Fenster des Tools wird angezeigt, ob der "Laufwerk klonen"-Modus aktiviert oder deaktiviert ist.

4. Um den Modus zum Klonen von Laufwerken zu deaktivieren, geben Sie in der Kommandozeile des Tools den folgenden Befehl ein:

   ```
   ./klmover -cloningmode 0
   ```

Installationseinstellungen für den Administrationsagenten

In der nachfolgenden Tabelle werden die MSI-Eigenschaften beschrieben, die bei der Installation des Administrationsagenten angepasst werden können. Alle Parameter mit Ausnahme von EULA und SERVERADDRESS sind optional.

Einstellungen für die Installation des Administrationsagenten im Silent-Modus

MSI-Eigenschaft	Beschreibung	Mögliche Werte
EULA	Einverständnis mit den Bedingungen des Lizenzvertrags	• 1 – Ich bestätige, dass ich die Bestimmungen und Bedingungen dieses Endbenutzer-Lizenzvertrags vollständig gelesen habe und sie verstehe und akzeptiere. • 0 – Ich lehne die Bedingungen des Endbenutzer-Lizenzvertrags ab (die Installation wird nicht ausgeführt). • Kein Wert – Ich lehne die Bedingungen des Endbenutzer-Lizenzvertrags ab (die Installation wird nicht ausgeführt).
DONT_USE_ANSWER_FILE	Installationseinstellungen aus der Antwortdatei lesen	• 1—Nicht verwenden. • Anderer Wert oder keine Angabe – Lesen.
INSTALLDIR	Pfad des Installationsordners für den Administrationsagenten	Zeichenfolgenwert.
SERVERADDRESS	Adresse des Administrationsservers (obligatorische Einstellung)	Zeichenfolgenwert.
SERVERPORT	Port zum Herstellen einer Verbindung mit dem Administrationsserver	Zahlenwert.
SERVERSSLPORT	Portnummer für das Herstellen einer sicheren Verbindung mit dem Administrationsserver über das SSL-Protokoll	Zahlenwert.
USESSL	Soll eine SSL-Verbindung verwendet werden?	• 1 – verwenden • Anderer Wert oder keine Angabe – nicht verwenden
OPENUDPPORT	Soll ein UDP-Port geöffnet werden?	• 1 – öffnen • Anderer Wert oder keine Angabe – öffnen
UDPPORT	UDP-Port	Zahlenwert.
USEPROXY	Soll ein Proxyserver verwendet werden?	• 1 – verwenden • Anderer Wert oder keine Angabe – nicht verwenden
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Proxyadresse und Portnummer für die Verbindung mit dem Proxyserver	Zeichenfolgenwert.
PROXYLOGIN	Benutzerkonto zur Verbindung mit dem Proxyserver.	Zeichenfolgenwert.
PROXYPASSWORD	Kennwort des Benutzerkontos für die Verbindung mit dem Proxyserver (Geben Sie in den Einstellungen von Installationspaketen keine Details über privilegierten Benutzerkonten an.)	Zeichenfolgenwert.
GATEWAYMODE	Modus für die Nutzung eines Verbindungs-Gateways	• 0 – Verbindungs-Gateway nicht verwenden • 1 – Als Verbindungs-Gateway wird der betreffende Administrationsagent verwendet • 2 – Verbindung mit dem Administrationsserver über das Verbindungs-Gateway herstellen

MSI-Eigenschaft	Beschreibung	Mögliche Werte
GATEWAYADDRESS	Verbindungs-Gateway-Adresse	Zeichenfolgenwert.
CERTSELECTION	Methode zum Anfordern eines Zertifikats	• GetOnFirstConnection – Zertifikat vom Administrationsserver anfordern • GetExistent – Vorhandenes Zertifikat auswählen. Wenn diese Variante ausgewählt ist, muss die Eigenschaft CERTFILE angegeben sein
CERTFILE	Pfad der Zertifikatsdatei	Zeichenfolgenwert.
VMVDI	Dynamischen Modus für Virtual Desktop Infrastructure (VDI) aktivieren	• 1 – aktivieren. • 0 – Nicht aktivieren. • Kein Wert – nicht aktivieren.
LAUNCHPROGRAM	Gibt an, ob nach der Installation der Dienst des Administrationsagenten gestartet werden soll. Bei "VMVDI=1" wird der Parameter ignoriert.	• 1 – starten • anderer Wert oder keine Angabe – nicht starten
NAGENTTAGS	Tag für den Administrationsagenten (hat eine höhere Priorität als das Tag aus der Antwortdatei)	Zeichenfolgenwert.

Anwendungen mit der Aufgabe zur Remote-Installation installieren

Mit Kaspersky Security Center Linux können Sie Anwendungen auf anderen Geräten per Fernzugriff installieren. Dazu dienen Aufgaben zur Remote-Installation. Mithilfe des Assistenten werden die Aufgaben erstellt und den Geräten zugewiesen. Um den Geräten schneller und einfacher eine Aufgabe zuzuweisen, können Sie die (bis zu 1.000) Geräte im Fenster des Assistenten auf die von Ihnen bevorzugte Art festlegen:

- **Aufgabe einer Administrationsgruppe zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Administrationsgruppe gehören.

- **Geräteadressen manuell angeben oder aus Liste importieren**. Sie können DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die Aufgabe zugewiesen werden soll.

- **Aufgabe einer Geräteauswahl zuweisen**. In diesem Fall wird die Aufgabe den Geräten zugewiesen, die zu einer zuvor erstellten Auswahl gehören. Sie können eine standardmäßig erstellte Auswahl oder Ihre eigene Auswahl angeben. Sie können maximal 1000 Geräte auswählen.

Um Probleme zu vermeiden, die während der Installation der Anwendung auf einem Client-Gerät ohne installierten Administrationsagent auftreten können, müssen Sie vorgehen, wie hier beschrieben: Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center Linux.

Über Aufgaben zur Remote-Installation in Kaspersky Security Center Linux

Kaspersky Security Center Linux bietet eine Vielzahl von Mechanismen zur Remote-Installation von Apps, die in Form von Aufgaben zur Remote-Installation der Apps realisiert werden (erzwungene Installation, Installation mithilfe des Kopierens Festplatten-Images). Die Aufgabe zur Remote-Installation kann sowohl für die angegebene Administrationsgruppe als auch für eine Reihe von Geräten oder für Geräteauswahlen erstellt werden (diese Aufgaben werden in der Kaspersky Security Center Web Console im Ordner **Aufgaben** angezeigt). Beim Erstellen der Aufgabe können die Installationspakete (des Administrationsagenten und/oder anderer Anwendungen) ausgewählt werden, die mithilfe der betreffenden Aufgabe installiert werden, sowie eine Reihe von Einstellungen festgelegt werden, mit denen die Art der Remote-Installation bestimmt wird. Darüber hinaus kann der Assistent für Remote-Installationen von Apps verwendet werden, dem das Erstellen der Aufgabe zur Remote-Installation von Apps und das Monitoring der Ergebnisse zugrunde liegt.

Aufgaben für Administrationsgruppen gelten nicht nur auf den Geräten, die zu dieser Gruppe gehören, sondern auch auf allen Geräte aller Untergruppen der ausgewählten Gruppe. Wenn in den Aufgabeneinstellungen die entsprechende Einstellung aktiviert ist, erstreckt sich die Aufgabe auf die Geräte der sekundären Administrationsserver, die sich in der betreffenden Gruppe oder ihren Untergruppen befinden.

Aufgaben für eine Reihe von Geräten aktualisieren die Liste der Client-Geräte bei jedem Start entsprechend der Zusammensetzung der Geräteauswahlen zum Zeitpunkt des Aufgabenstarts. Wenn sich in der Geräteauswahl Geräte befinden, die mit sekundären Administrationsservern verbunden sind, wird die Aufgabe auch auf diesen Geräten ausgeführt. Details über diese Einstellungen und die Installationsmethoden werden in diesem Abschnitt beschrieben.

Für die erfolgreiche Ausführung der Aufgabe zur Remote-Installation auf Geräten, die mit sekundären Administrationsserver verbunden sind, müssen die von der Aufgabe verwendeten Installationspakete vorher mithilfe der Aufgabe zur Relaisübertragung an die entsprechenden sekundären Administrationsserver weitergeleitet werden.

Eines Programm remote installieren

Dieser Abschnitt enthält Informationen darüber, wie eine Anwendung auf Geräten in einer Administrationsgruppe, auf Geräten mit bestimmten Adressen oder auf einer Auswahl an Geräten remote installiert wird.

Um eine Anwendung auf ausgewählten Geräten zu installieren:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie im Feld **Aufgabentyp** die Variante **Remote-Installation einer Anwendung** aus.

4. Wählen Sie eine der folgenden Varianten aus:

- **Aufgabe einer Administrationsgruppe zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

  Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

  Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

- **Geräteadressen manuell angeben oder aus Liste importieren**

  Sie können DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die Aufgabe zugewiesen werden soll.

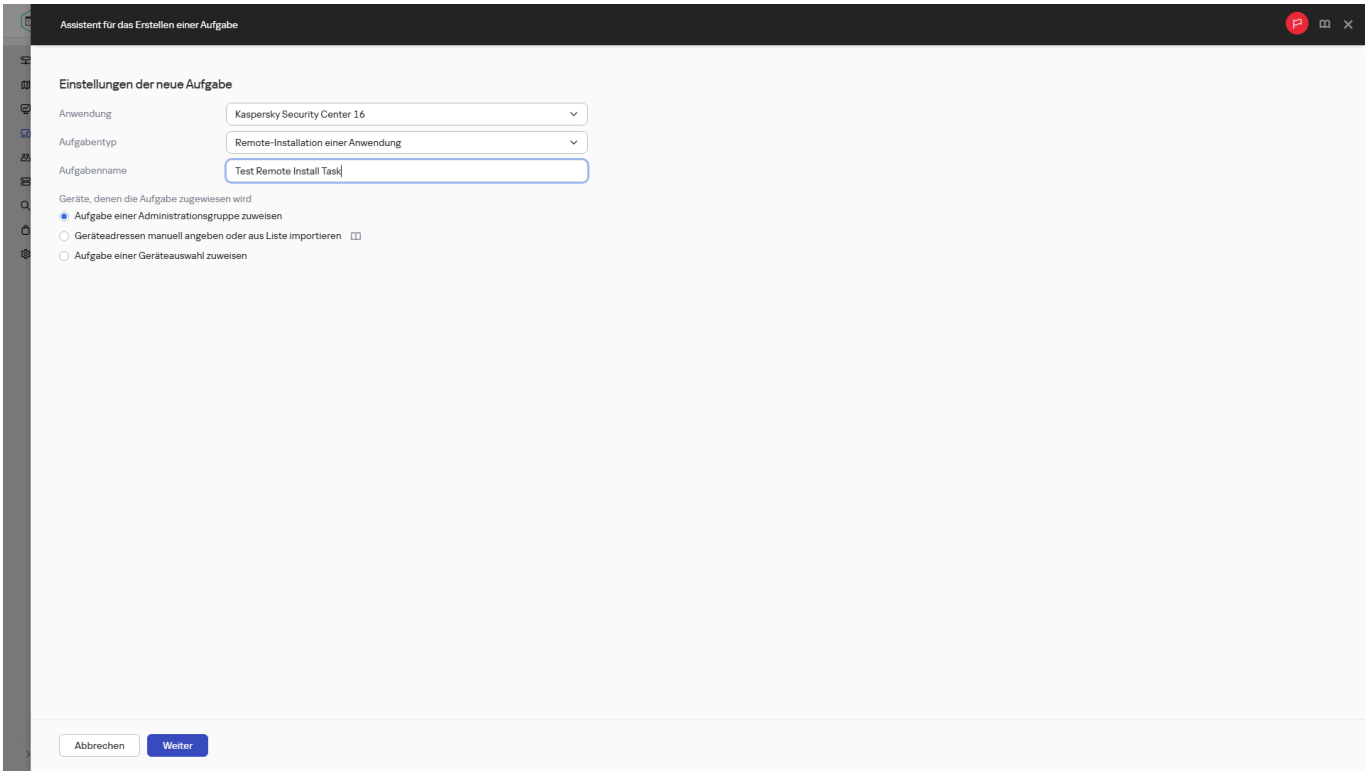
  Diese Option können Sie beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

Die Aufgabe *Remote-Installation einer Anwendung* wird für die angegebenen Geräte erstellt. Wenn Sie Option **Aufgabe einer Administrationsgruppe zuweisen** ausgewählt haben, ist die Aufgabe eine Gruppenaufgabe.



Erstellen der Aufgabe Remote-Installation einer Anwendung

5. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Auswahl an Geräten an.

   Die verfügbaren Einstellungen hängen von der im vorherigen Schritt ausgewählten Option ab.

6. Geben Sie im Schritt **Installationspakete** die folgenden Einstellungen an:

   - Wählen Sie im Feld **Installationspaket auswählen** das Installationspaket einer Anwendung, die Sie installieren möchten.

   - Wählen Sie in der Einstellungsgruppe **Download des Installationspakets erzwingen** die Methode der Übertragung der zur Anwendungsinstallation erforderlichen Dateien auf die Client-Geräte aus:

     - **Unter Nutzung des Administrationsagenten**

       Wenn die Option aktiviert ist, werden die Installationspakete von dem auf den Client-Geräten installierten Administrationsagenten zugestellt.

       Wenn diese Option deaktiviert ist, werden Installationspakete mithilfe der Betriebssystems-Tools der Client-Geräte ausgeliefert.

       Es wird empfohlen, die Option zu aktivieren, wenn die Aufgabe für Geräte mit installierten Administrationsagenten vorgesehen ist.

       Diese Option ist standardmäßig aktiviert.

     - **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**

       Wenn diese Option aktiviert ist, werden Installationspakete mithilfe der Tools von den Betriebssystemen durch Verteilungspunkte auf die Geräte übertragen. Diese Variante ist wählbar, wenn sich im Netzwerk mindestens ein Verteilungspunkt befindet.

       Ist die Option **Mithilfe des Administrationsagenten** aktiviert, werden die Dateien nur dann mit den Betriebssystem-Tools zugestellt, wenn die Funktionen des Administrationsagenten nicht verwendet werden können.

       Standardmäßig ist diese Option für die Aufgaben von Remote-Installationen aktiviert, die auf einem virtuellen Administrationsserver erstellt wurden.

       Die einzige Möglichkeit, eine Windows-Anwendung (einschließlich Administrationsagent für Windows) auf einem Gerät zu installieren, auf dem kein Administrationsagent installiert ist, besteht in der Verwendung eines Windows-basierten Verteilungspunkts. Wenn Sie daher eine Windows-Anwendung installieren wollen:

       - Wählen Sie diese Option.

       - Stellen Sie sicher, dass den Ziel-Client-Geräten ein Verteilungspunkt zugewiesen ist.

       - Stellen Sie sicher, dass der Verteilungspunkt Windows-basiert ist.

     - **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**

       Wenn diese Option aktiviert ist, werden die Dateien durch den Administrationsserver mittels Betriebssystem-Tools der Client-Gerät auf die Client-Geräte übertragen. Diese Option kann aktiviert werden, wenn auf dem Client-Gerät kein Administrationsagent installiert ist, das Client-Gerät sich aber im selben Netzwerk wie der Administrationsserver befindet.

       Diese Option ist standardmäßig aktiviert.

   - Geben Sie im Feld **Maximale Anzahl gleichzeitiger Downloads** die erlaubte Maximalanzahl an Client-Geräten, an die der Administrationsserver simultan Dateien ausliefern kann.

- Geben Sie im Feld **Maximale Anzahl der Installationsversuche** die maximal zulässige Anzahl von gestarteten Installationsvorgängen an.

  Wenn die im Parameter angegebene Anzahl an Versuchen überschritten wird, startet Kaspersky Security Center Linux das Installationsprogramm auf dem Gerät nicht mehr. Um die Aufgabe *Remote-Installation einer Anwendung* erneut zu starten, erhöhen Sie den Wert für den Parameter **Maximale Anzahl der Installationsversuche** und starten Sie die Aufgabe erneut. Alternativ dazu können Sie eine neue Aufgabe zur *Remote-Installation einer Anwendung* erstellen.

- Wenn Sie von einer Kaspersky-Sicherheitsanwendung auf eine andere migrieren möchten und die aktuelle Anwendung durch ein Kennwort geschützt ist, geben Sie das Kennwort in dem Feld **Deinstallationskennwort der aktuellen Kaspersky-Anwendung** ein Beachten Sie, dass Ihre aktuelle Kaspersky-Anwendung während der Migration deinstalliert wird.

  Das Feld **Deinstallationskennwort der aktuellen Kaspersky-Anwendung** ist nur verfügbar, wenn Sie die Option **Unter Nutzung des Administrationsagenten** in der Einstellungsgruppe **Download des Installationspakets erzwingen** ausgewählt haben.

  Sie können das Deinstallationskennwort nur für das Migrationsszenario von Kaspersky Security für Windows Server auf Kaspersky Endpoint Security für Windows verwenden, wenn Sie Kaspersky Endpoint Security für Windows mithilfe der Aufgabe zur Remote-Installation von Programmen installieren. Die Verwendung des Deinstallationskennworts bei der Installation anderer Komponenten kann zu Installationsfehlern führen.

  Um das Migrationsszenario erfolgreich abzuschließen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

  - Sie verwenden Kaspersky Security Center Administrationsagent 14.2 für Windows oder höher.
  - Sie installieren das Programm auf Geräten mit Microsoft Windows.

- Passen Sie die erweiterte Einstellung an:

  - **Anwendung nicht neu installieren, wenn sie bereits installiert ist**

    Wenn diese Option aktiviert ist, wird die ausgewählte Anwendung nicht neu installiert, wenn es bereits auf dem Client-Gerät installiert ist.

    Wenn Sie dieses Kontrollkästchen deaktivieren, wird die Anwendung in jedem Fall installiert.

    Diese Option ist standardmäßig aktiviert.

  - **Typ des Betriebssystems vor dem Download überprüfen**

    Bevor die Dateien auf die Client-Geräte übertragen werden, überprüft Kaspersky Security Center Linux, ob die Einstellungen des Installations-Hilfsprogramms auf dem Betriebssystem des Client-Geräts anwendbar sind. Wenn die Einstellungen nicht anwendbar sind, überträgt Kaspersky Security Center Linux die Dateien nicht und wird nicht versuchen, die Anwendung zu installieren. So können Sie beispielsweise eine Anwendung auf den Geräten einer Administrationsgruppe, die mehrere Geräte mit unterschiedlichen Betriebssystemen enthält, installieren, indem Sie die Aufgabe zur Installation der Administrationsgruppe zuweisen und anschließend die Option zum Überspringen von Geräten mit davon abweichenden Betriebssystemen aktivieren.

Wenn Sie den Administrationsagenten per Remote-Installation auf nicht zugeordneten Geräten installieren, bestimmt Kaspersky Security Center Linux oder ein Verteilungspunkt das Betriebssystem des Geräts automatisch, unabhängig davon, welchen Wert die Einstellung **Typ des Betriebssystems vor dem Download überprüfen** hat.

- **Installation des Pakets in Active Directory-Gruppenrichtlinien zuweisen**

  Wenn diese Option aktiviert ist, wird das Installationspaket mithilfe von Richtlinien des Active Directory installiert.

  Die Option ist verfügbar, wenn ein Installationspaket des Administrationsagenten ausgewählt ist.

  Diese Option ist standardmäßig deaktiviert.

- **Benutzer auffordern, laufende Anwendungen zu schließen**

  Laufende Anwendungen können das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

- Wählen Sie aus, auf welchen Geräten Sie die Anwendung installieren möchten:

  - **Auf allen Geräten installieren**

    Wird die Anwendung selbst auf den Geräten installiert, die von anderen Administrationsservern verwaltet werden.

    Diese Variante ist standardmäßig festgelegt. Sie müssen diese Einstellung nicht ändern, wenn Sie nur einen Administrationsserver in Ihrem Netzwerk haben.

  - **Nur auf Geräten installieren, die durch diesen Administrationsserver verwaltet werden**

    Wird die Anwendung nur auf den Geräten installiert, die von diesem Administrationsserver verwaltet werden. Wählen Sie diese Option, wenn Sie in Ihrem Netzwerk mehrere Administrationsserver haben und Konflikte zwischen diesen vermeiden möchten.

- Geben Sie an, ob die Geräte nach Abschluss der Installation in eine Administrationsgruppe verschoben werden müssen:

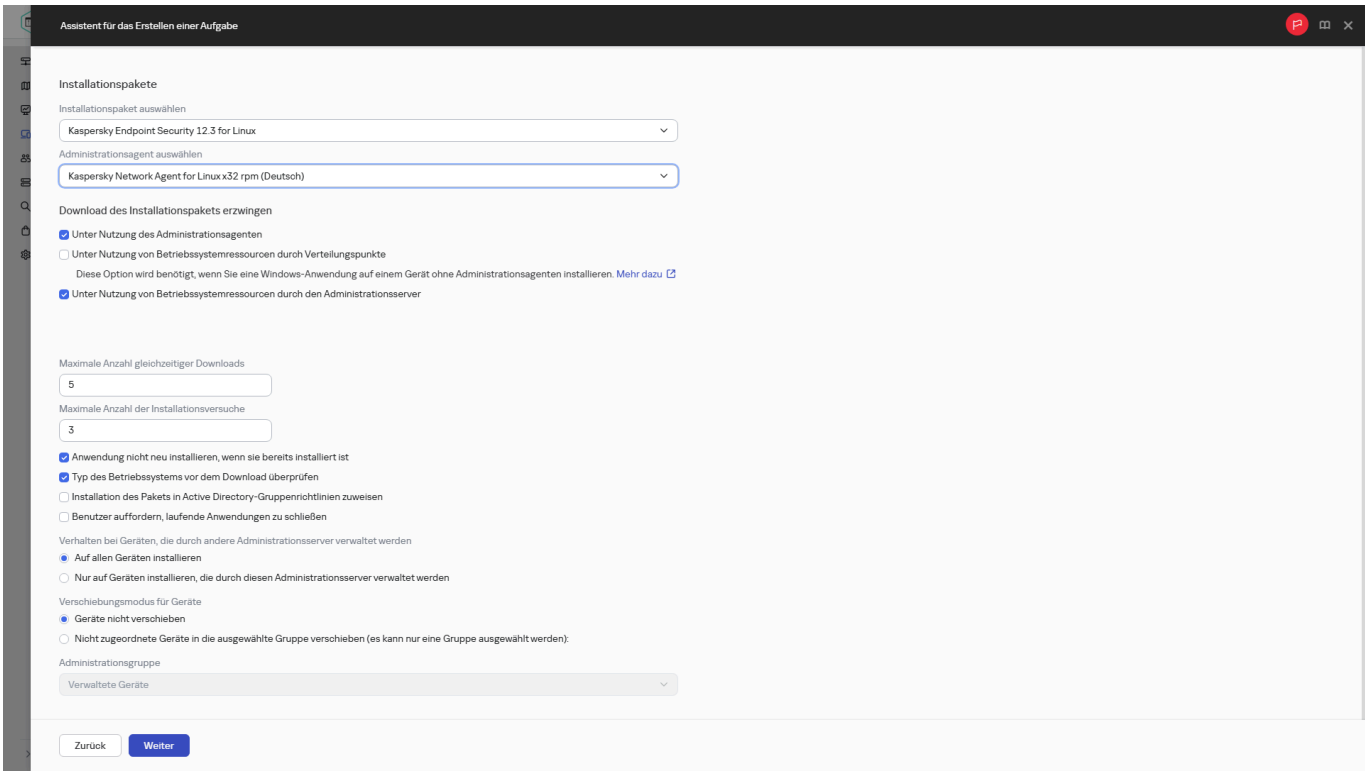
  - **Geräte nicht verschieben**

    Die Geräte bleiben in den Gruppen, in denen sie sich gerade befinden. Die Geräte, die keiner Gruppe zugeordnet wurden, bleiben nicht zugeordnet.

  - **Nicht zugeordnete Geräte in die ausgewählte Gruppe verschieben (es kann nur eine Gruppe ausgewählt werden)**

    Die Geräte werden in die ausgewählte Administrationsgruppe verschoben.

  Beachten Sie, dass die Option **Geräte nicht verschieben** standardmäßig festgelegt ist. Aus Sicherheitsgründen sollten Sie die Geräte manuell verschieben.



Angeben der Aufgabeneinstellungen

7. Geben Sie in diesem Schritt des Assistenten an, ob die Geräte während der Installation von Anwendungen neu gestartet werden sollen:

   - **Gerät nicht neu starten**

     Bei dieser Option wird das Gerät nach der Installation der Sicherheitsanwendung nicht neu gestartet.

   - **Gerät neu starten**

     Bei dieser Option wird das Gerät nach der Installation der Sicherheitsanwendung neu gestartet.

8. Bei Bedarf können Sie im Schritt **Benutzerkonten für den Zugriff auf Geräte auswählen** die Konten hinzufügen, die zum Start der Aufgabe *Remote-Installation einer Anwendung* verwendet werden sollen:

   - **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**

     Wenn diese Variante ausgewählt ist, muss das Benutzerkonto nicht angegeben werden, unter dem das Installationsprogramm der Anwendung gestartet werden soll. Die Aufgabe wird unter dem Konto gestartet, unter dem der Dienst des Administrationsservers läuft.

     Wenn der Administrationsagent nicht auf den Client-Geräten installiert ist, steht diese Option nicht zur Verfügung.

- **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)**

  Wählen Sie diese Option, wenn auf den Geräten, denen Sie die Aufgabe zur Remote-Installation zuweisen, der Administrationsagent nicht installiert ist. In diesem Fall können Sie ein Benutzerkonto oder ein SSH-Zertifikat angeben, um die Anwendung zu installieren.

  - **Lokales Konto oder Domänenkonto**. Wenn Sie diese Variante auswählen, können Sie das Benutzerkonto angeben, unter dem das Installationsprogramm gestartet werden soll. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Lokales Konto oder Domänenkonto** aus, und geben Sie anschließend die Anmeldeinformationen des Benutzerkontos an.

    Sie können mehrere Benutzerkonten angeben, wenn beispielsweise kein Benutzerkonto existiert, dass über die erforderlichen Rechte auf allen Geräten verfügt, für welche die Aufgabe bestimmt wurde. In diesem Fall werden für den Start der Aufgabe alle hinzugefügten Konten nacheinander von oben nach unten angewandt.

  - **SSH-Zertifikat**. Wenn Sie eine Anwendung auf einem Linux-basierten Client-Gerät installieren möchten, können Sie anstelle eines Benutzerkontos ein SSH-Zertifikat angeben. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **SSH-Zertifikat** aus, und geben Sie anschließend den privaten und den öffentlichen Schlüssel des Zertifikats an.

    Um einen privaten Schlüssel zu generieren, können Sie das Tool "ssh-keygen" verwenden. Beachten Sie, dass die Kaspersky Security Center Linux das pem-Format für private Schlüssel verwendet, das Tool "ssh-keygen" jedoch standardmäßig SSH-Schlüssel im OpenSSH-Format generiert. Das OpenSSH-Format wird von Kaspersky Security Center Linux nicht unterstützt. Um einen privaten Schlüssel im unterstützten pem-Format zu erstellen, fügen Sie die dem Befehl "ssh-keygen" den Parameter "-m PEM" hinzu. Beispielsweise:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "< Benutzer-E-Mail >"
    ```

9. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um die Aufgabe zu erstellen und den Assistenten zu beenden.

   Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen, ändern oder bei Bedarf einen Startzeitplan für die Aufgabe konfigurieren.

10. Wählen Sie in der Aufgabenliste die von Ihnen erstellte Aufgabe aus und klicken Sie anschließend auf **Start**.

    Alternativ können Sie warten, bis die Aufgabe nach dem in den Aufgabeneinstellungen festgelegten Zeitplan gestartet wird.

Nach Abschluss der Remote-Installationsaufgabe wurde die ausgewählte Anwendung auf den angegebenen Geräten installiert.

Remote-Installation von Anwendungen auf macOS-Geräten

So installieren Sie Anwendungen auf Geräten mit macOS mithilfe einer Aufgabe zur Remote-Installation:

1. Erstellen Sie ein Archiv, das aus einem Installationspaket und einem .sh-Installationsskript besteht.

2. Deaktivieren Sie im Assistenten für das Erstellen einer Aufgabe die Option **Typ des Betriebssystems vor dem Download überprüfen**.

Alternativ können Sie die Aufgabe **Skripte remote ausführen** verwenden. Im folgenden Artikel wird beschrieben, wie Sie Dateien für diese Aufgabe konfigurieren: Remote-Installation von Programmen auf Geräten mithilfe der Aufgabe zur Remote-Ausführung von Skripten.

Anwendungen auf sekundären Administrationsservern installieren

Wenn Ihr Administrationsserver Version 15.4 oder höher ist, können Sie Anwendungen nur auf einem sekundären Administrationsserver installieren, wenn dessen Version 15.4 oder höher ist.

Um eine Anwendung auf sekundären Administrationsservern zu installieren:

1. Stellen Sie eine Verbindung zum Administrationsserver her, der die gewünschten sekundären Administrationsserver verwaltet.

2. Vergewissern Sie sich, dass sich das zur Anwendung passende Installationspaket auf jedem der gewählten sekundären Administrationsserver befindet. Wenn Sie das Installationspaket auf keinem der sekundären Server finden können, verteilen Sie es. Erstellen Sie dazu eine Aufgabe mit dem Aufgabentyp **Installationspaket verteilen**.

3. Erstellen Sie eine Aufgabe zur Remote-Installation der Anwendung auf den sekundären Administrationsservern. Wählen Sie den Aufgabentyp **Remote-Installation einer Anwendung auf sekundärem Administrationsserver** aus.

   Der Assistent für das Erstellen einer Aufgabe erstellt eine Aufgabe, mit der die im Assistenten ausgewählte Anwendung per Fernzugriff auf den angegebenen sekundären Administrationsservern installiert werden kann.

4. Starten Sie die Aufgabe manuell oder warten Sie, bis die Aufgabe nach dem in den Aufgabeneinstellungen festgelegten Zeitplan gestartet wird.

Nach Abschluss der Remote-Installationsaufgabe wurde die ausgewählte Anwendung auf den angegebenen sekundären Administrationsservern installiert.

Remote-Installation von Apps auf Geräte mit installiertem Administrationsagenten

Wenn auf dem Gerät ein arbeitsfähiger Administrationsagent installiert ist, der mit dem primären Administrationsserver oder einen seiner sekundären Server verbunden ist, kann auf diesem Gerät die Version des Administrationsagenten aktualisiert werden sowie mithilfe des Administrationsagenten beliebige unterstützte Apps installiert, aktualisiert oder gelöscht werden.

Sie können Option **Unter Nutzung des Administrationsagenten** in den Eigenschaften der Aufgabe zur Remote-Installation aktivieren.

Wenn diese Option ausgewählt ist, erfolgt die Übertragung der Installationspakete auf die Geräte mit den vom Administrator festgelegten Installationseinstellungen über die Verbindungskanäle zwischen dem Administrationsagenten und dem Administrationsserver.

Zur Optimierung der Belastung auf dem Administrationsserver und zur Verringerung des Datenverkehrs zwischen dem Administrationsserver und den Geräten ist es sinnvoll, in jedem Remote-Netzwerk bzw. in jeder Broadcast-Domäne Verteilungspunkte zu bestimmen (s. Abschnitte Über Verteilungspunkte und Aufbau der Struktur von Administrationsgruppen und Zuweisung von Verteilungspunkten). In diesem Fall erfolgt die Verteilung der Installationspakete und der Einstellungen des Installers vom Administrationsserver auf die Geräte über die Verteilungspunkte.

Unter Verwendung der Verteilungspunkte können auch Broadcast-Domänen (Multicast) den Mailversand der Installationspakete ausführen, wodurch der Netzwerkverkehr während der Bereitstellung der Programme erheblich verringert werden kann.

Bei der Übertragung der Installationspakete auf die Geräte über die Verbindungskanäle zwischen den Administrationsagenten und dem Administrationsserver, werden die zur Sendung vorbereiteten Installationspakete zusätzlich im Ordner "/var/opt/kaspersky/klnagent_srv/1093/.working/" zwischengespeichert. Bei Verwendung einer hohen Anzahl verschiedener Installationspakete mit großem Umfang und bei einer großen Menge von Verteilungspunkten kann die Größe dieses Ordners erheblich zunehmen.

Die Dateien aus dem Ordner FTServer dürfen nicht manuell gelöscht werden. Beim Löschen der Ausgangsinstallationspakete werden die entsprechenden Daten automatisch aus dem Ordner FTServer gelöscht.

Die von den Verteilungspunkten empfangenen Daten werden im Ordner "/var/opt/kaspersky/klnagent_srv/1103/" gespeichert.

Die Dateien aus dem Ordner FTCITmp dürfen nicht manuell gelöscht werden. Je nach Abschluss der Aufgaben, von denen die Daten aus dem Ordner verwendet werden, wird der Inhalt dieses Ordners automatisch gelöscht.

Da die Installationspakete im für das Netzwerk optimalen Format für die Übertragung über die Verbindungskanäle zwischen dem Administrationsserver und den Administrationsagenten aus dem Zwischenspeicher bewegen, dürfen keine Änderungen an den Installationspaketen im ursprünglichen Ordner des Installationspakets vorgenommen werden. Solche Änderungen werden vom Administrationsserver nicht automatisch berücksichtigt. Wenn die Dateien der Installationspakete manuell geändert werden müssen (obwohl das nicht empfohlen wird), müssen unbedingt irgendwelche Einstellungen des Installationspakets in der Kaspersky Security Center Web Console geändert werden. Die Änderung der Einstellungen des Installationspakets in der Kaspersky Security Center Web Console zwingt den Administrationsserver, das Image des Pakets im Cache zu aktualisieren, das für die Sendung auf die Geräte vorbereitet wurde.

Während der Remote-Installation sendet der Server ICMP-Echo-Anfragen (entspricht dem Befehl "ping") an das Zielgerät.

Verwaltung des Neustarts von Geräten in der Aufgabe zur Remote-Installation

Oft wird für den Abschluss der Remote-Installation der App (besonders auf der Plattform Windows) ein Neustart des Geräts gefordert.

Wenn die Aufgabe zur Remote-Installation von Kaspersky Security Center Linux verwendet wird, kann im Assistenten für das Erstellen einer Aufgabe oder im Eigenschaftenfenster der erstellten Aufgabe (Abschnitt **Neustart des Betriebssystems**) die Maßnahme für einen erforderlichen Neustart ausgewählt werden:

- **Gerät nicht neu starten**. In diesem Fall wird kein automatischer Neustart ausgeführt. Für das Abschließen der Installation ist es erforderlich, das Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung der Geräte) neu zu starten. Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Installationsaufgaben auf Servern und anderen Geräten, für die Störungen während des Arbeitsablaufs kritisch sind.

- **Das Gerät neu starten**. In diesem Fall wird der Neustart immer automatisch ausgeführt, wenn für das Abschließen der Installation ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben zur Installation auf Geräten, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**. In diesem Fall informiert eine Meldung auf dem Client-Gerät den Benutzer darüber, dass das Gerät manuell neu gestartet werden muss. Für diese Variante können einige erweiterten Einstellungen definiert werden: Text der Nachricht für den Benutzer, die Anzeigehäufigkeit der Nachricht, sowie die Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Die Variante **Benutzer fragen** eignet sich besonders für Workstations, deren Benutzer die Möglichkeit haben sollen, den passendsten Moment für den Neustart auszuwählen.

Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center Linux

Um die erstmalige Bereitstellung des Administrationsagenten oder von anderen Anwendungen durchzuführen, können Sie die Installation der ausgewählten Installationspakete mithilfe der Aufgabe zur Remote-Installation von Kaspersky Security Center Linux erzwingen. Voraussetzung dafür ist jedoch, dass jedes Gerät über mindestens ein Benutzerkonto mit lokalen Administratorrechten verfügt.

Die erzwungene Installation kann auch verwendet werden, falls die Geräte nicht unmittelbar für den Administrationsserver verfügbar sind: wenn sich die Geräte beispielsweise in isolierten Netzwerken befinden oder wenn sich die Geräte im lokalen Netzwerk befinden und der Administrationsserver in der demilitarisierten Zone befindet.

Im Falle einer erstmaligen Bereitstellung ist noch kein Administrationsagent installiert. Daher können Sie in den Einstellungen der Aufgabe zur Remote-Installation nicht die Option auswählen, die zur Installation der Anwendung benötigten Dateien mithilfe des Administrationsagent zu verteilen. Sie können die Dateien lediglich unter Verwendung der Betriebssystemressourcen durch den Administrationsserver und die Verteilungspunkte verteilen.

Auf den Zielgeräten muss der Dienst des Administrationsservers unter einem Benutzerkonto mit Administratorrechten ausgeführt werden. Alternativ können Sie in den Einstellungen der Aufgabe zur Remote-Installation ein Benutzerkonto angeben, das Zugriff auf die Freigabe "admin$" hat.

Standardmäßig wird Aufgabe zur Remote-Installation auf Geräte angewendet, indem die Anmeldedaten des Benutzerkontos, unter dem der Administrationsserver ausgeführt wird, verwendet werden. Es ist wichtig, zu beachten, dass es sich dabei um das Konto mit dem Zugriff auf die Freigabe "admin$" handelt, und nicht um das Konto, unter dem die Aufgabe zur Remote-Installation ausgeführt wird. Die Installation wird unter dem Benutzerkonto "LocalSystem" ausgeführt.

Angeben können Sie die Geräte entweder explizit (mittels Liste), indem Sie die Administrationsgruppe von Kaspersky Security Center Linux auswählen, in der die Geräte enthalten sind, oder durch das Erstellen einer Geräteauswahl nach bestimmten Bedingungen. Der Startzeitpunkt der Installation wird durch den Zeitplan der Aufgabe bestimmt. Wenn in den Eigenschaften der Aufgabe die Einstellung **Übersprungene Aufgaben starten** aktiviert ist, kann die Aufgabe sofort bei der Aktivierung der Geräte oder bei ihrer Übertragung in die Ziel-Administrationsgruppe ausgeführt werden.

Die erzwungene Installation erfolgt mittels Übertragung der Installationspakete an die Zielgeräte, dem anschließenden Kopieren der Dateien in die admin$-Ressource der jeweiligen Geräte und der Remote-Anmeldung der Hilfsdienste auf diesen Geräten. Die Übertragung der Installationspakete an die Zielgeräte wird mithilfe der für die Netzwerkinteraktion verantwortlichen Funktion von Kaspersky Security Center Linux ausgeführt. Dabei müssen die folgenden Bedingungen erfüllt werden:

- Die Zielgeräte können sowohl vom Administrationsserver als auch von den Verteilungspunkten erreicht werden.
- Die Namensauflösung für die Zielgeräte funktioniert im Netzwerk fehlerfrei.
- Die freigegebenen Administratorressourcen (admin$) verbleiben auf den Zielgeräten aktiviert.
- Die folgenden Systemdienste werden auf Zielgeräten ausgeführt:
  - Server (LanmanServer)

    Dieser Dienst wird standardmäßig ausgeführt.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- Der TCP-Port 445 ist auf den Zielgeräten geöffnet, um Remote-Zugriff über die Windows Management Instrumentation (WMI) zu ermöglichen.

  > TCP 139, UDP 137 und UDP 138 werden von älteren Protokollen verwendet und sind für aktuelle Anwendungen nicht mehr erforderlich.

  Um den Administrationsserver und die Verteilungspunkte mit den Zielgeräten zu verbinden, müssen in der Firewall dynamische Zugriffsports für ausgehende Daten erlaubt sein.
- Die Sicherheitseinstellungen der Active Directory-Domänenrichtlinie erlauben die Verwendung des NTLM-Protokolls während der Bereitstellung des Administrationsagenten.
- Auf Zielgeräten mit Microsoft Windows XP ist die einfache Dateifreigabe deaktiviert.

- Auf den Zielgeräten ist das Zugriffs- und Sicherheitsmodell auf den Wert *Klassisch – lokale Benutzer authentifizieren sich selbst* eingestellt. Der Wert *Nur Gäste – lokale Benutzer authentifizieren sich als Gast* ist nicht zulässig.

- Die Geräte sind Mitglieder der Domäne oder auf den Geräten wurden bereits einheitliche Benutzerkonten mit Administratorrechten erstellt.

Für die erfolgreiche Bereitstellung des Administrationsagenten oder einer anderen Anwendungen auf einem Gerät, das keiner Active Directory-Domäne von Windows Server 2003 oder höher gehört, müssen Sie die Remote-UAC auf diesem Gerät deaktivieren. Unter anderem aufgrund von Remote-UAC ist es lokalen Administratorkonten nicht möglich, auf die Freigabe "admin$" zuzugreifen. Für die erzwungene Bereitstellung des Administrationsagenten oder anderer Anwendungen ist dieser Zugriff ist jedoch erforderlich. Das Deaktivieren von Remote-UAC hat keine Auswirkungen auf die lokale UAC.

Bei der Installation auf neuen Geräten, die noch nicht in die Administrationsgruppen von Kaspersky Security Center Linux verschoben wurden, kann in den Eigenschaften der Aufgabe zur Remote-Installation die Administrationsgruppe festgelegt werden, in welche die Geräte verschoben werden, nachdem die Installation des Administrationsagenten auf ihnen abgeschlossen wurde.

Beim Erstellen der Gruppenaufgabe muss berücksichtigt werden, dass die Gruppenaufgabe für die Geräte aller angelegten Untergruppen der ausgewählten Gruppe gilt. Deshalb sollten doppelte Installationsaufgaben in den Untergruppen vermieden werden.

Eine vereinfachte Methode zur Erstellung von Aufgaben für eine erzwungene Installation von Anwendungen ist die automatische Installation. Dazu müssen Sie in den Eigenschaften der Administrationsgruppe in der Liste der Installationspakete jene Pakete auswählen, die auf den Geräten dieser Gruppe installiert werden sollen. Daraufhin werden auf allen Geräten dieser Gruppe und ihrer Untergruppen die ausgewählten Installationspakete automatisch installiert. Der Zeitraum, während dem die Pakete installiert werden, hängt von der Netzwerkfähigkeit und der Gesamtmenge der Geräte im Netzwerk ab.

Um die Belastung des Administrationsservers während der Übertragung der Installationspaketen an die Zielgeräte zu reduzieren, können Sie in der Installationsaufgabe die Installationsmethode über Verteilungspunkte auswählen. Beachten Sie dabei, dass diese Installationsmethode eine höhere Belastung für jene Geräte bedeutet, die als Verteilungspunkte agieren. Es wird daher empfohlen, Geräte auszuwählen, die den Voraussetzungen für Verteilungspunkte entsprechen. Sie müssen bei der Verwendung von Verteilungspunkten sicherstellen, dass diese sich in all jenen isolierten Subnetzen befinden, in denen Zielgeräte gehostet werden.

Die Nutzung der Verteilungspunkte als lokale Installationszentren kann auch für die Installation auf Geräten in Subnetzen bequem sein, die mit dem Administrationsserver über einen engen Verbindungskanal verbunden sind, während zwischen den Geräten innerhalb des Subnetzes ein breiter Verbindungskanal verfügbar ist.

Die Größe des freien Speicherplatzes auf der Partition, in der sich der Ordner "/var/opt/kaspersky/KSC_Backups*" befindet, muss den Gesamtumfang der Programmpakete der installierten Anwendungen um ein Vielfaches übertreffen.

Programme im Silent-Modus installieren

Um ein Programm im nicht Silent-Modus zu installieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung** → **Installationspakete**.

2. Aktivieren Sie das Kontrollkästchen neben dem Installationspaket der gewünschten Anwendung oder erstellen Sie ein neues Paket für diese Anwendung.

   Das Installationspaket wird auf dem Administrationsserver im gemeinsamen Ordner im Dienstordner Packages gespeichert. Jedem Installationspaket entspricht dabei der jeweilige Unterordner.

3. Öffnen Sie den Ordner des gewünschten Installationspakets auf eine der folgenden Arten:

   - Kopieren Sie den Ordner, der zum gewünschten Installationspaket passt, vom Administrationsserver auf das Client-Gerät. Öffnen Sie danach den kopierten Ordner auf dem Client-Gerät.

   - Öffnen Sie anschließend vom Client-Gerät aus den gemeinsamen Ordner auf dem Administrationsserver, der zum gewünschten Installationspaket passt.

   Wenn sich der freigegebene Ordner auf einem Gerät befindet, auf dem Microsoft Windows Vista installiert ist, müssen Sie den **Deaktiviert-Wert** für die Benutzerkontensteuerung festlegen: Führen Sie **alle Administratoren im Administratorbestätigungsmodus aus** (**Start** → **Systemsteuerung** → **Verwaltung** → **Lokale Sicherheitsrichtlinie** → **Sicherheitseinstellungen**).

4. Je nach dem gewählten Programm gehen Sie wie folgt vor:

   - Bei Kaspersky Anti-Virus für Windows Workstation, Kaspersky Anti-Virus für Windows Server und Kaspersky Security Center wechseln Sie in den Unterordner exec und starten Sie die ausführbare Datei (mit der Erweiterung .exe) mit dem Parameter /s.

   - Bei den übrigen Kaspersky-Anwendungen starten Sie aus dem geöffneten Ordner die ausführbare Datei (mit der Erweiterung .exe) mit dem Schlüssel /s.

   Der Start einer ausführbaren Datei mit den Parametern `EULA=1` und `PRIVACYPOLICY=1` bedeutet, dass Sie die Bedingungen des Endbenutzer-Lizenzvertrags und der Datenschutzrichtlinie vollständig gelesen haben, und sie verstehen und akzeptieren. Außerdem wissen Sie, dass Ihre Daten, wie in der Datenschutzrichtlinie beschrieben, verarbeitet und übertragen werden (einschließlich in Drittländer). Der Text des Lizenzvertrags und der Text der Datenschutzrichtlinie sind im Lieferumfang von Kaspersky Security Center Linux enthalten. Die Annahme der Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie ist die Voraussetzung für die Installation oder das Update des Programms.

Ein Gerät mit dem Betriebssystem macOS für die Remote-Installation des Administrationsagenten vorbereiten

Die folgenden Methoden stehen zur erstmaligen Installation des Administrationsagenten auf einem verwalteten macOS-Gerät zur Verfügung:

- Durch Ausführen der Aufgabe zur Remote-Installation auf einem macOS-basierten Verteilungspunkt.
- Indem Sie den Gerätebenutzern Links zu den autonomen Paketen schicken, die von Kaspersky Security Center Linux erstellt wurden. Autonomen Pakete sind ausführbare Module, in denen die Programmpakete der ausgewählten Programme mit den konfigurierten Einstellungen enthalten sind.

Um ein Gerät mit dem Betriebssystem macOS für die Remote-Installation des Administrationsagenten vorzubereiten, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass sudo auf dem macOS-Zielgerät installiert ist.
2. Testen Sie die Konfiguration des Geräts:
   a. Stellen Sie sicher, dass auf dem Client-Gerät der Port 22 geöffnet ist. Um dies zu tun, öffnen Sie in den **Systemeinstellungen** den Bereich **Teilen** und stellen Sie anschließend sicher, dass das Kontrollkästchen **Fernanmeldung** aktiviert ist.

      Sie können sich mittels Secure Shell (SSH) nur über Port 22 mit dem Client-Gerät verbinden. Sie können die Portnummer nicht ändern.

      Sie können den Befehl `ssh <Gerätename>` verwenden, um sich entfernt auf dem macOS-Gerät anzumelden. Im Reiter **Freigaben** können Sie die Option **Auswahl der anmeldeberechtigten Benutzer** verwenden, um die Benutzer festzulegen, denen der Zugriff auf das macOS-Gerät gewährt werden soll.

   b. Deaktivieren Sie das Kennwort der sudo-Abfrage für das Benutzerkonto, das für die Verbindung mit dem Gerät verwendet wird.

      Verwenden Sie den `sudo visudo`-Befehl, um die sudoers-Konfigurationsdatei zu öffnen. Geben Sie in der geöffneten Datei unter dem Eintrag `User privilege specification` folgendes an: `username ALL = (ALL) NOPASSWD: ALL`. In diesem Fall steht `username` für ein Benutzerkonto, das für die Verbindung mit dem Gerät über das SSH-Protokoll verwendet wird.

   c. Speichern und schließen Sie die Datei sudoers.

   d. Stellen Sie erneut eine Verbindung zum Gerät über SSH her und stellen Sie mithilfe des Befehls `sudo whoami` sicher, dass der Sudo-Dienst kein Kennwort abfragt.

3. Laden Sie das Installationspaket herunter und erstellen Sie es:

    a. Laden Sie das Installationspaket des Administrationsagenten mittels einer der folgenden Methoden herunter:

    - Über die Programmoberfläche
    - Indem Sie die benötigte Version des Administrationsagenten von der Website des Technischen Supports unter https://support.kaspersky.com/de herunterladen
    - Durch das Anfordern des Installationspakets von den Spezialisten des Technischen Supports

    b. Verwenden Sie folgende Dateien, um ein Installationspaket für Remote-Installation zu erstellen:

    - klnagent.kud
    - install.sh
    - klnagentmac.dmg

4. Erstellen Sie eine Aufgabe zur Remote-Installation des Programms mit den folgenden Einstellungen:

- Wählen Sie auf der Seite **Einstellungen** des Assistenten für das Erstellen einer Aufgabe das Kontrollkästchen **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**. Deaktivieren Sie alle anderen Kontrollkästchen.
- Um die Aufgabe auszuführen, geben Sie auf der Seite **Benutzerkonto für die Ausführung der Aufgabe auswählen** die Benutzerkonto-Einstellungen an, die für die Verbindung mit dem Gerät über SSH verwendet werden.

Das Client-Gerät ist zur Remote-Installation des Administrationsagenten über die von Ihnen erstellte entsprechende Aufgabe bereit.

Virtuelle Infrastruktur

Kaspersky Security Center Linux unterstützt die Verwendung von virtuellen Maschinen. Sie können den Administrationsagenten und die Sicherheitsanwendungen auf jeder virtuellen Maschine installieren und virtuelle Maschinen auf Hypervisor-Ebene schützten. Im ersten Fall kann sowohl die Standard-Sicherheitsanwendung als auch Kaspersky Security for Virtualization Light Agent für den Schutz der virtuellen Maschinen verwendet werden. Im zweiten Fall kann Kaspersky Security for Virtualization Agentless verwendet werden.

Kaspersky Security Center Linux unterstützt das Rollback von virtuellen Maschinen auf ihren vorherigen Zustand.

Empfehlungen zur Senkung der Belastung auf den virtuellen Maschinen

Wenn der Administrationsagent auf einer virtuellen Maschine installiert wird, muss eine Möglichkeit zum Deaktivieren jenes Teils der Funktionalität von Kaspersky Security Center Linux vorgesehen werden, der für die virtuellen Maschinen von geringem Wert ist.

Bei der Installation des Administrationsagenten auf einer virtuellen Maschine oder einer Vorlage, aus der virtuelle Maschinen erstellt werden sollen, ist es empfehlenswert, wie folgt vorzugehen:

- Wenn eine Remote-Installation ausgeführt wird, wählen Sie im Eigenschaftenfenster für das Installationspaket des Administrationsagenten im Abschnitt **Erweitert** die Option **Einstellungen für VDI optimieren** aus.
- Wenn mithilfe des Assistenten eine interaktive Installation ausgeführt wird, wählen Sie im Fenster des Assistenten die Option **Einstellungen des Administrationsagenten für die virtuelle Infrastruktur optimieren** aus.

Durch Auswählen der Optionen werden die Einstellungen des Administrationsagenten so geändert, dass standardmäßig die folgenden Funktionen deaktiviert werden (bevor eine Richtlinie angewendet wird):

- Informationen über die installierte Software empfangen
- Informationen über die Hardware empfangen
- Informationen über vorhandene Schwachstellen empfangen
- Informationen über erforderliche Updates empfangen

Üblicherweise müssen die aufgezählten Funktionen auf den virtuellen Maschinen nicht aktiviert sein, damit die Software und die virtuelle Hardware darauf einheitlich sind.

Das Deaktivieren der Funktionen kann rückgängig gemacht werden. Wenn eine der deaktivierten Funktionen doch erforderlich ist, kann sie mithilfe der Richtlinie des Administrationsagenten oder in den lokalen Einstellungen des Administrationsagenten aktiviert werden. Die lokalen Einstellungen des Administrationsagenten sind über das Kontextmenü des entsprechenden Geräts in der Kaspersky Security Center Web Console verfügbar.

Unterstützung von dynamischen virtuellen Maschinen

Kaspersky Security Center Linux unterstützt dynamische virtuelle Maschinen. Wenn im Netzwerk des Unternehmens eine virtuelle Infrastruktur implementiert ist, können in einigen Fällen dynamische (temporärer) virtuellen Maschinen verwendet werden. Solche Maschinen werden mit eindeutigen Namen aus einer vom Administrator im Voraus vorbereiteten Vorlage erstellt. Der Benutzer arbeitet eine gewisse Zeit auf einer VM und nach dem Deaktivieren wird die virtuelle Maschinen aus der virtuellen Infrastruktur entfernt. Wenn im Netzwerk des Unternehmens Kaspersky Security Center Linux implementiert ist, wird die virtuelle Maschine mit darauf installiertem Administrationsagenten zur Administrationsserver-Datenbank hinzugefügt. Nach dem Deaktivieren der virtuellen Maschine muss der sie betreffende Eintrag auch aus der Administrationsserver-Datenbank gelöscht werden.

Damit die Funktionalität des automatischen Löschens der Einträge über virtuelle Maschinen bei der Installation des Administrationsagenten auf der Vorlage, aus der die dynamischen virtuellen Maschinen erstellt werden, funktioniert, muss die Option **Dynamischen Modus für VDI aktivieren** aktiviert werden:

- Im Falle einer Remote-Installation im Eigenschaftenfenster des Installationspakets des Administrationsagenten (Abschnitt **Erweitert**)
- Für die interaktive Installation – im Installationsassistenten des Administrationsagenten

Die Option **Dynamischen Modus für VDI aktivieren** muss bei der Installation des Administrationsagenten auf realen Geräten nicht aktiviert werden.

Wenn es erforderlich ist, dass Ereignisse auf dynamischen virtuellen Maschinen eine bestimmte Zeit nach dem Löschen der Maschinen auf dem Administrationsserver gespeichert werden, muss im Eigenschaftenfenster des Administrationsservers im Abschnitt **Ereignis-Datenverwaltung** die Option **Ereignisse von gelöschten Geräten weiterhin speichern** aktiviert und die maximale Speicherdauer der Ereignisse in Tagen angegeben werden.

Es wird davon abgeraten, die Verschlüsselung von Laufwerken auf dynamischen virtuellen Maschinen zu aktivieren.

Unterstützung des Kopierens von virtuellen Maschinen

Das Kopieren von virtuellen Maschine mit darauf installiertem Administrationsagenten oder deren Erstellung aus einer Vorlage mit installiertem Administrationsagenten entspricht der Bereitstellung der Administrationsagenten durch Aufzeichnen und Kopieren eines Festplatten-Image. Deshalb muss man im Allgemeinen beim Kopieren von virtuellen Maschinen dieselbe Aktion ausführen wie bei der Bereitstellung des Administrationsagenten durch Kopieren eines Images der Festplatte.

In den nachstehend beschriebenen beiden Fällen erkennt der Administrationsagent die Tatsache des Kopierens allerdings automatisch. Deshalb ist die Ausführung der komplizierten Aktionen, die in im Abschnitt "die Bereitstellung durch Aufzeichnen und Kopieren der Festplatte des Geräts" nicht obligatorisch:

- Bei der Installation des Administrationsagenten war die Option **Dynamischen Modus für VDI aktivieren** aktiviert: nach jedem Neustart des Betriebssystems wird eine solche virtuelle Maschine unabhängig von der Tatsache, dass sie kopiert wurde, als neues Gerät betrachtet.

- Es wird einer der folgenden Hypervisoren verwendet: VMware™, HyperV oder Xen: der Administrationsagent erkennt die Tatsache des Kopierens der virtuellen Maschine anhand der geänderten ID der virtuellen Hardware.

Die Analyse der Änderungen der virtuellen Hardware ist nicht absolut sicher. Bevor die vorliegende Methode umfassend verwendet wird, muss zuvor ihre Funktionsfähigkeit für die im Unternehmen verwendete Version des Hypervisors auf einer kleinen Anzahl virtueller Maschinen geprüft werden.

Einstellungen für die Remote-Installation auf Unix-Geräten angeben

Wenn Sie eine Anwendung mithilfe einer Aufgabe zur Remote-Installation auf einem Unix-Gerät installieren, können Sie Unix-spezifische Einstellungen für die Aufgabe angeben. Diese Einstellungen sind in den Aufgabeneigenschaften verfügbar, nachdem die Aufgabe erstellt wurde.

So geben Sie Unix-spezifische Einstellungen für eine Aufgabe zur Remote-Installation an:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.

2. Klicken Sie auf den Namen der Aufgabe zur Remote-Installation, für die Sie die Unix-spezifischen Einstellungen festlegen möchten.

   Das Fenster mit den Aufgabeneigenschaften wird geöffnet.

3. Gehen Sie zu **Anwendungseinstellungen** → **Unix-spezifische Einstellungen**.

4. Geben Sie die folgenden Einstellungen an:

   - **Legen Sie ein Kennwort für das Root-Benutzerkonto fest (nur für Bereitstellungen mittels SSH)**

     Wenn der Befehl `sudo` auf dem Zielgerät nicht verwendet werden kann, ohne das Kennwort anzugeben, wählen Sie diese Option aus und geben Sie dann das Kennwort für das Root-Benutzerkonto an. Kaspersky Security Center Linux überträgt das Kennwort in verschlüsselter Form an das Zielgerät, entschlüsselt das Kennwort und startet dann im Namen des Root-Benutzerkontos mit dem angegebenen Kennwort den Installationsvorgang.

     > Kaspersky Security Center Linux verwendet das Benutzerkonto oder das angegebene Kennwort nicht, um eine SSH-Verbindung herzustellen.

   - **Geben Sie den Pfad eines temporären Ordners an, der sich auf dem Zielgerät befindet und die "Execute"-Berechtigung besitzt (nur für Bereitstellungen mittels SSH)**

     Wenn das Verzeichnis /tmp auf dem Zielgerät nicht über die Ausführungsberechtigung verfügt, wählen Sie diese Option aus und geben Sie den Pfad des Verzeichnisses mit der Ausführungsberechtigung an. Kaspersky Security Center Linux verwendet das angegebene Verzeichnis als temporäres Verzeichnis für den Zugriff über SSH. Die Anwendung legt das Installationspaket in dem Verzeichnis ab und führt den Installationsvorgang aus.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert.

Monitoring der Bereitstellung

Um die Bereitstellung von Kaspersky Security Center Linux zu überwachen und sicherzustellen, dass auf den verwalteten Geräten eine Sicherheitsanwendung und ein Administrationsagent installiert sind, verwenden Sie die Funktion Überwachung und Berichterstattung:

- Mit dem Widget "Bereitstellung" des Dashboards können Sie die Bereitstellung in Echtzeit zu überwachen.
- Verwenden Sie Berichte, um detaillierte Informationen abzurufen.

Kaspersky-Anwendung starten und beenden

Mit der Aufgabe *Anwendung starten oder beenden* können Sie Kaspersky-Anwendungen auf verwalteten Geräten starten und beenden.

So erstellen Sie eine Aufgabe zum Starten oder Beenden von Anwendungen:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.

3. Wählen Sie in der Dropdown-Liste **Anwendung** die Anwendung aus, für welche Sie die Aufgabe erstellen möchten.

   In der Liste werden Kaspersky-Anwendungen angezeigt, wenn Sie bereits Verwaltungs-Web-Plug-ins für diese Anwendungen hinzugefügt haben.

4. Wählen Sie in der Liste **Aufgabentyp** die Aufgabe **Anwendungsaktivierung** aus.

5. Geben Sie im Feld **Aufgabenname** den Namen der neuen Aufgabe an.

   Der Aufgabenname darf höchstens 100 Zeichen lang sein und darf keine Sonderzeiten ("*<>?\:|) enthalten.

6. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.

7. Gehen Sie im Fenster **Anwendungen** wie folgt vor:

   - Aktivieren Sie die Kontrollkästchen neben den Namen der Anwendungen, für die Sie die Aufgabe erstellen möchten.
   - Wählen Sie die Option **Anwendung starten** oder **Anwendung beenden**.

8. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** im Schritt **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

10. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

11. Geben Sie im Fenster mit den Aufgabeneigenschaften die allgemeinen Aufgabeneinstellungen an und speichern Sie anschließend die Einstellungen.

Die Aufgabe wird erstellt und konfiguriert.

Wenn Sie die Aufgabe ausführen möchten, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf **Starten**.

Sicherheitsanwendungen von Drittanbietern ersetzen

Zur Installation der Sicherheitsanwendungen von Kaspersky mithilfe von Kaspersky Security Center Linux ist es möglicherweise erforderlich, Drittanbieter-Programme zu löschen, die mit der zu installierenden Anwendung nicht kompatibel ist. Kaspersky Security Center Linux bietet mehrere Methoden zur Deinstallation von Drittanbieter-Anwendungen.

Inkompatible Anwendungen während der Konfiguration der Remote-Installation einer Anwendung entfernen

Sie können die Option **Inkompatible Anwendungen automatisch entfernen** aktivieren, wenn Sie die Remote-Installation einer Sicherheitsanwendung im Assistenten für die Bereitstellung des Schutzes konfigurieren. Wenn diese Option aktiviert ist, entfernt Kaspersky Security Center Linux vor der Installation einer Sicherheitsanwendung auf dem verwalteten Gerät inkompatible Anwendungen.

Löschen der inkompatiblen Anwendungen mithilfe einer separaten Aufgabe

Zum Löschen der inkompatiblen Anwendungen wird die Aufgabe *Remote-Deinstallation einer Anwendung* verwendet. Die Aufgabe muss vor der Aufgabe zur Installation der Sicherheitsanwendung auf den Geräten gestartet werden. Beispielsweise kann in der Installationsaufgabe ein Zeitplan des Typs **Nach Beenden einer anderen Aufgabe** ausgewählt werden, wobei die andere Aufgabe die Aufgabe *Remote-Deinstallation einer Anwendung* ist.

Die Verwendung dieser Löschmethode ist zweckmäßig, wenn der Installer der Sicherheitsanwendung eine der inkompatiblen Anwendungen nicht erfolgreich löschen kann.

Programme oder Software-Updates remote löschen

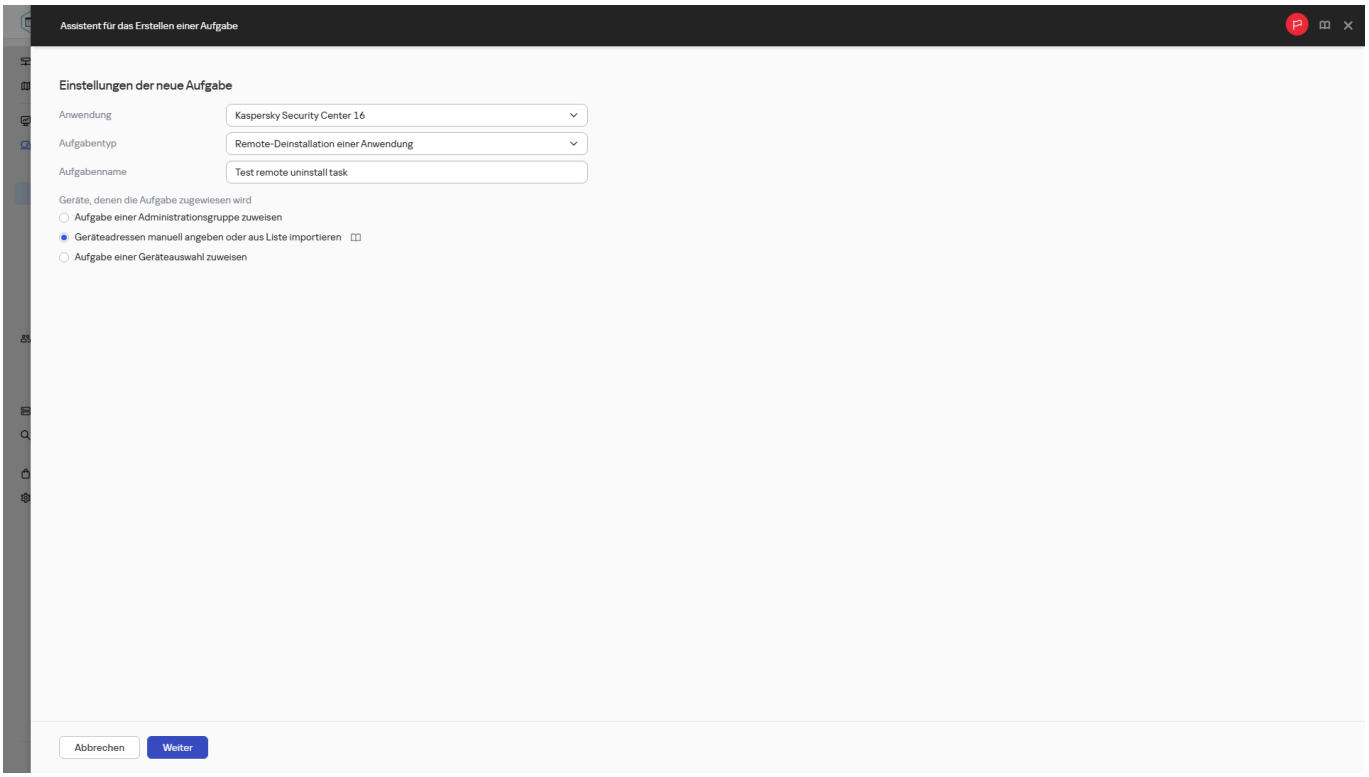
Sie können Anwendungen oder Programm-Updates auf verwalteten Geräten, auf denen Linux ausgeführt wird, per Fernzugriff nur über den Administrationsagenten entfernen.

Um Anwendungen oder Programm-Updates von ausgewählten Geräten remote zu entfernen:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.
3. Wählen Sie in der Dropdown-Liste **Anwendung** die Option "Kaspersky Security Center" aus.
4. Wählen Sie in der Liste **Aufgabentyp** den Typ **Remote-Deinstallation einer Anwendung** aus.
5. Geben Sie im Feld **Aufgabenname** den Namen der neuen Aufgabe an.

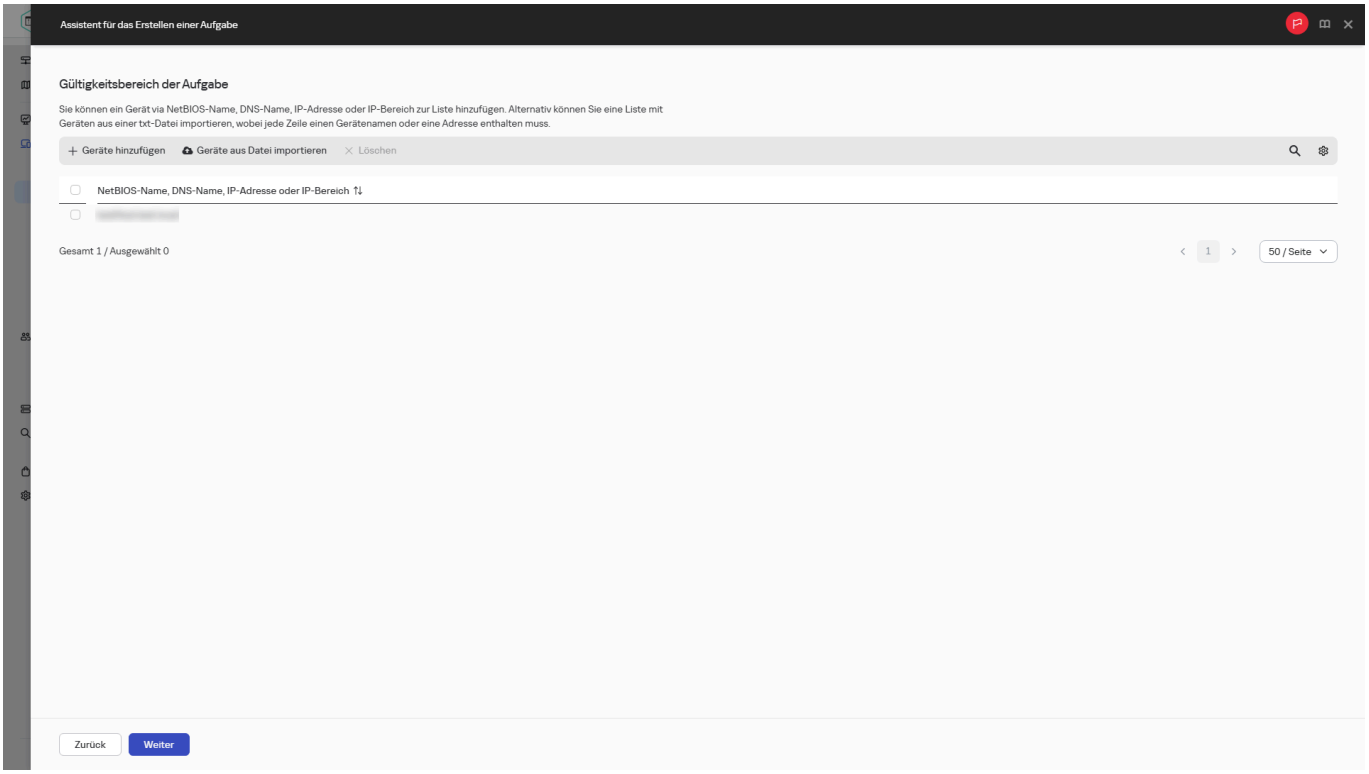
   Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.



Erstellen der Aufgabe Remote-Deinstallation einer Anwendung

6. Wählen Sie die Geräte, denen die Aufgabe zugewiesen werden soll.

   Wechseln Sie zum nächsten Schritt des Assistenten.



Angeben des Gültigkeitsbereichs der Aufgabe

7. Wählen Sie aus, welche Art von Software Sie entfernen wollen, und wählen Sie anschließend bestimmte Anwendungen, Updates oder Patches aus, die Sie entfernen wollen:

   - **Verwaltete Anwendung deinstallieren**

     Eine Liste mit Kaspersky-Anwendungen wird angezeigt. Wählen Sie die Anwendung aus, die Sie entfernen möchten.

   - **Inkompatibles Anwendung deinstallieren**

     Eine Liste der Anwendungen, die nicht mit Kaspersky-Sicherheitsanwendungen oder Kaspersky Security Center Linux kompatibel sind, wird angezeigt. Aktivieren Sie die Kontrollkästchen neben den Anwendungen, die Sie entfernen möchten.

   - **Anwendung aus der Programm-Registry deinstallieren**

     Standardmäßig übertragen Administrationsagenten die Information über Anwendungen, die auf verwalteten Geräten installiert sind, an den Administrationsserver. Die Liste der installierten Anwendungen wird in der Programm-Registry gespeichert.

     So wählen Sie eine Anwendung aus der Programm-Registry aus:

     a. Klicken Sie auf das Feld **Zu deinstallierende Anwendung** und wählen Sie anschließend die Anwendung aus, die Sie entfernen wollen.

     Wenn Sie beim Ausführen der Aufgabe das Programm "Kaspersky Security Center Administrationsagent" auswählen, zeigt der Status *Erfolgreich abgeschlossen* an, dass der Deinstallationsvorgang gestartet wurde. Nach dem Löschen des Kaspersky Security Center Administrationsagenten ändert sich der Status nicht. Wenn die Aufgabe fehlschlägt, ändert sich der Status in *Fehlgeschlagen*.

b. Geben Sie die folgenden Optionen für die Deinstallation an:

- **Deinstallationsmodus**

  Wählen Sie aus, wie Sie die Anwendung entfernen möchten:

  - **Deinstallationsbefehl automatisch bestimmen**

    Wenn die Anwendung einen Deinstallationsbefehl besitzt, der durch den Hersteller der Anwendung vorgegeben wurde, nutzt Kaspersky Security Center Linux diesen Befehl. Es wird empfohlen, diese Option zu aktivieren.

  - **Deinstallationsbefehl angeben**

    Wählen Sie diese Option aus, wenn Sie einen eigenen Befehl für die Deinstallation der Anwendung angeben möchten.

    > Es wird empfohlen, das Entfernen der Anwendung zunächst unter Verwendung der Option **Deinstallationsbefehl automatisch bestimmen** auszuprobieren. Sollte die Deinstallation mit dem automatisch definierten Befehl fehlschlagen, verwenden Sie einen eigenen Befehl.

    Geben Sie einen Installationsbefehl in das Feld ein und geben Sie danach die folgende Option an:

    Diesen Deinstallationsbefehl nur dann verwenden, wenn der Standardbefehl nicht automatisch bestimmt werden konnte

    Kaspersky Security Center Linux prüft, ob die ausgewählte Anwendung einen vom Hersteller der Anwendung vorgegeben Deinstallationsbefehl besitzt. Wenn ein solcher Befehl existiert, verwendet Kaspersky Security Center Linux diesen anstelle des Befehls der im Feld **Deinstallationsbefehl der Anwendung** angegeben ist.

    Es wird empfohlen, diese Option zu aktivieren.

- **Gerät nach erfolgreicher Deinstallation der Anwendung neu starten**

  Wenn die Anwendung nach einer erfolgreichen Deinstallation einen Neustart des Betriebssystems auf dem verwalteten Gerät erfordert, wird das Betriebssystem automatisch neu gestartet.

- **Bestimmtes Anwendungs-Update, einen Patch oder Drittherstelleranwendung deinstallieren**

  Es wird eine Liste mit Updates, Patches und Drittanbieter-Anwendungen angezeigt. Wählen Sie das Objekt aus, das Sie entfernen möchten.

  Die angezeigte Liste ist eine allgemeine Liste mit Anwendungen und Updates, die nicht den tatsächlich installierten Anwendungen und Updates auf den verwalteten Geräten entspricht. Es wird empfohlen, vor der Auswahl eines Objekts zu überprüfen, ob die Anwendung oder das Update tatsächlich auf dem im Aufgabenbereich festgelegten Geräten installiert ist. Sie können sich die Liste mit Geräten, auf denen die Anwendung oder das Update installiert ist, über das Eigenschaftenfenster anzeigen lassen.

  So zeigen Sie die Liste der Geräte an:

  a. Klicken Sie auf den Namen der Anwendung oder des Updates.

     Daraufhin wird das Eigenschaftenfenster geöffnet.

  b. Öffnen Sie den Abschnitt **Geräte**.

     Sie können sich die Liste mit installierten Anwendungen und Updates auch im Eigenschaftenfenster des Geräts ansehen.

8. Geben Sie an, auf welche Weise die Client-Geräte das Deinstallations-Hilfsprogramm herunterladen sollen:

- **Unter Nutzung des Administrationsagenten**

  Die Dateien werden den Client-Geräten mithilfe des Administrationsagenten, der auf den Geräten installiert ist, ausgeliefert.

  Wenn diese Option deaktiviert ist, werden die Dateien über Tools des Linux-Betriebssystems ausgeliefert.

  Es wird empfohlen, die Option zu aktivieren, wenn die Aufgabe für Geräte mit installierten Administrationsagenten vorgesehen ist.

- **Unter Nutzung von Betriebssystemressourcen durch den Administrationsserver**

  Diese Option ist veraltet. Verwenden Sie stattdessen die Option **Unter Nutzung des Administrationsagenten** oder **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**.

  Die Dateien werden mit den Tools des Betriebssystems über den Administrationsserver an die Client-Geräte übertragen. Diese Option kann aktiviert werden, wenn auf dem Client-Gerät kein Administrationsagent installiert ist, das Client-Gerät sich aber im selben Netzwerk wie der Administrationsserver befindet.

- **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**

  Die Dateien werden mit Tools des Betriebssystems über Verteilungspunkte an die Client-Geräte ausgeliefert. Diese Option kann aktiviert werden, wenn sich mindestens ein Verteilungspunkt im Netzwerk befindet.

  Ist die Option **Unter Nutzung des Administrationsagenten** aktiviert, werden die Dateien nur dann mit den Tools des Betriebssystems zugestellt, wenn die Funktionen des Administrationsagenten nicht verwendet werden können.

- **Maximale Anzahl gleichzeitiger Downloads**

  Die erlaubte Höchstzahl an Client-Geräten, an die der Administrationsserver simultan Dateien ausliefern kann. Je höher die Nummer, umso schneller werden die Anwendungen deinstalliert, aber umso höher ist auch die Auslastung des Administrationsservers.

- **Maximale Anzahl der Deinstallationsversuche**

  Wenn es Kaspersky Security Center Linux nicht gelingt, eine Anwendung im Rahmen der Aufgabe *Remote-Deinstallation einer Anwendung* unter Einhaltung der maximalen Anzahl von Deinstallationsversuchen auf einem verwalteten Gerät zu deinstallieren, beendet Kaspersky Security Center Linux die Auslieferung des Deinstallationstools an dieses verwaltete Gerät und startet die Installationsaufgabe auf dem Gerät nicht mehr.

  Mit dem Parameter **Maximale Anzahl der Deinstallationsversuche** können Sie die Ressourcen eines verwalteten Geräts schonen und den Datenverkehr reduzieren (Deinstallation, MSI-Datei ausführen und Fehlermeldungen).

  Wiederkehrende Versuche zum Aufgabestart können auf ein Problem auf dem Gerät hinweisen, das die Deinstallation verhindert. Der Administrator sollte das Problem innerhalb der angegebenen Anzahl an Deinstallationsversuchen lösen und die Aufgabe anschließend neu starten (manuell oder mittels Zeitplan).

  Wenn die Deinstallation nicht abgeschlossen werden kann, ist das Problem unter Umständen nicht lösbar und jeder weitere Aufgabenstart wäre ein unnützer Verbrauch von Ressourcen und Datenverkehr.

  Beim Erstellen der Aufgabe wird der Zähler für Versuche auf `0` gesetzt. Jede Ausführung des Installationsprogramms, die einen Fehler zurückgibt, erhöht den Zählerstand.

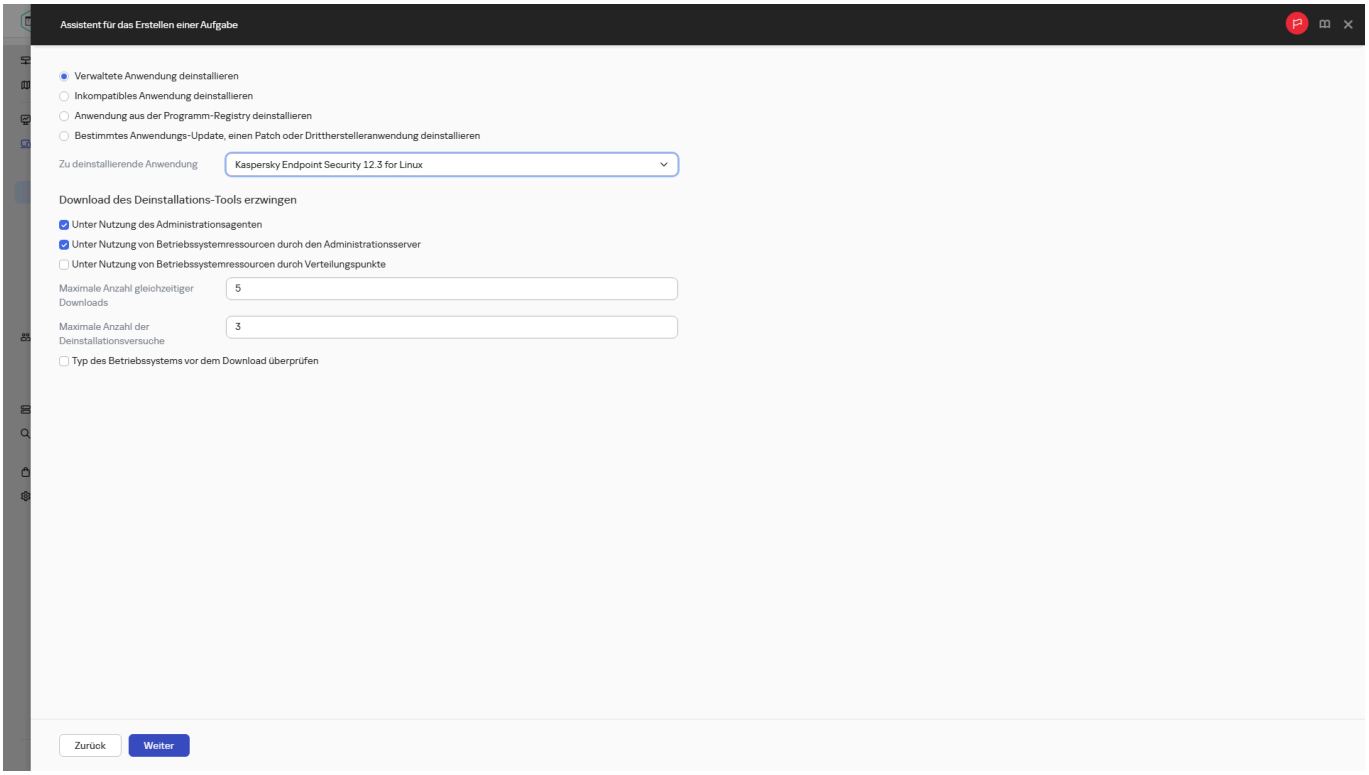
Wenn die im Parameter angegebene Anzahl an Versuchen überschritten wurde und das Gerät für die Deinstallation der Anwendung bereit ist, können Sie den Wert **Maximale Anzahl der Deinstallationsversuche** erhöhen und die Deinstallations-Aufgabe starten. Alternativ können Sie eine neue Aufgabe des Typs *Remote-Deinstallation einer Anwendung* erstellen.

- **Typ des Betriebssystems vor dem Download überprüfen**

  Bevor die Dateien auf die Client-Geräte übertragen werden, überprüft Kaspersky Security Center Linux, ob die Einstellungen des Installations-Hilfsprogramms auf dem Betriebssystem des Client-Geräts anwendbar sind. Wenn die Einstellungen nicht anwendbar sind, überträgt Kaspersky Security Center Linux die Dateien nicht und wird nicht versuchen, die Anwendung zu installieren. So können Sie beispielsweise eine Anwendung auf den Geräten einer Administrationsgruppe, die mehrere Geräte mit unterschiedlichen Betriebssystemen enthält, installieren, indem Sie die Aufgabe zur Installation der Administrationsgruppe zuweisen und anschließend die Option zum Überspringen von Geräten mit davon abweichenden Betriebssystemen aktivieren.

  Wenn Sie den Administrationsagenten per Remote-Installation auf nicht zugeordneten Geräten installieren, bestimmt Kaspersky Security Center Linux oder ein Verteilungspunkt das Betriebssystem des Geräts automatisch, unabhängig davon, welchen Wert die Einstellung **Typ des Betriebssystems vor dem Download überprüfen** hat.

Gehen Sie zum nächsten Schritt des Assistenten.



Angeben der Aufgabeneinstellungen

9. Geben Sie Neustart-Einstellungen des Betriebssystems an:

- **Gerät nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

- **Gerät neu starten**

  Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Option ist standardmäßig ausgewählt.

  - **Aufforderung wiederholen alle (Min.)**

  - **Neu starten nach (Min.)**

- **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

Gehen Sie zum nächsten Schritt des Assistenten.

10. Bei Bedarf können Sie Benutzerkonten hinzufügen, die für den Start der Aufgabe zur Remote-Deinstallation verwendet werden sollen:

    - **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**

      Wenn diese Variante ausgewählt ist, muss das Benutzerkonto nicht angegeben werden, unter dem das Installationsprogramm der Anwendung gestartet werden soll. Die Aufgabe wird unter dem Konto gestartet, unter dem der Dienst des Administrationsservers läuft.

      Wenn der Administrationsagent nicht auf den Client-Geräten installiert ist, steht diese Option nicht zur Verfügung.

- **Benutzerkonto erforderlich (Administrationsagent wird nicht verwendet)**

  Wählen Sie diese Option, wenn auf den Geräten, denen Sie die Aufgabe zur *Remote-Deinstallation* zuweisen, der Administrationsagent nicht installiert ist. In diesem Fall können Sie ein Benutzerkonto oder ein SSH-Zertifikat angeben, um die Anwendung zu deinstallieren.

  - **Lokales Konto oder Domänenkonto**. Wenn Sie diese Variante auswählen, können Sie das Benutzerkonto angeben, unter dem das Installationsprogramm gestartet werden soll. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Lokales Konto oder Domänenkonto** aus, und geben Sie anschließend die Anmeldeinformationen des Benutzerkontos an.

    Sie können mehrere Benutzerkonten angeben, wenn beispielsweise kein Benutzerkonto existiert, dass über die erforderlichen Rechte auf allen Geräten verfügt, für welche die Aufgabe bestimmt wurde. In diesem Fall werden für den Start der Aufgabe alle hinzugefügten Konten nacheinander von oben nach unten angewandt.

  - **SSH-Zertifikat**. Wenn Sie eine Anwendung von einem Linux-basierten Client-Gerät deinstallieren möchten, können Sie anstelle eines Benutzerkontos ein SSH-Zertifikat angeben. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **SSH-Zertifikat** aus, und geben Sie anschließend den privaten und den öffentlichen Schlüssel des Zertifikats an.

    Um einen privaten Schlüssel zu generieren, können Sie das Tool "ssh-keygen" verwenden. Beachten Sie, dass die Kaspersky Security Center Linux das pem-Format für private Schlüssel verwendet, das Tool "ssh-keygen" jedoch standardmäßig SSH-Schlüssel im OpenSSH-Format generiert. Das OpenSSH-Format wird von Kaspersky Security Center Linux nicht unterstützt. Um einen privaten Schlüssel im unterstützten pem-Format zu erstellen, fügen Sie die dem Befehl "ssh-keygen" den Parameter "-m PEM" hinzu.

    Beispielsweise:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<Benutzer-E-Mail>"
    ```

11. Aktivieren Sie im Schritt **Erstellung der Aufgabe abschließen** des Assistenten die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**, um die standardmäßigen Aufgabeneinstellungen zu ändern.

    Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später ändern.

12. Klicken Sie auf die Schaltfläche **Fertigstellen**.

    Der Assistent erstellt die Aufgabe. Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit Aufgabeneigenschaften automatisch geöffnet. In diesem Fenster können Sie die allgemeinen Aufgabeneinstellungen angeben und bei Bedarf die bei der Aufgabenerstellung festgelegten Einstellungen ändern.

    > Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Aufgabenliste auf den Namen der erstellten Aufgabe klicken.

    Die Aufgabe wurde erstellt, konfiguriert und wird in der Aufgabenliste unter **Aufgaben** angezeigt.

13. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf **Starten**.

    Auf der Registerkarte **Zeitplan** im Eigenschaftenfenster der Aufgabe können Sie auch einen Zeitplan für den Aufgabenstart festlegen.

    Eine genaue Beschreibung der Einstellungen für den Start nach Zeitplan finden Sie in den allgemeinen Aufgabeneinstellungen.

Nachdem Abschluss der Aufgabe wurde die ausgewählte Anwendung von allen ausgewählten Geräten deinstalliert.

Probleme bei der Remote-Deinstallation

Es kann passieren, dass bei der Remote-Deinstallation einer Drittanbieter-Anwendung die folgende Warnung angezeigt wird: "Die Remote-Deinstallation wurde auf diesem Gerät mit Warnungen abgeschlossen: Die zu entfernende Anwendung ist nicht installiert." Dieses Problem tritt auf, wenn die zu deinstallierende Anwendung bereits deinstalliert wurde oder nur für einen einzelnen Benutzer installiert ist. Anwendungen, die für einen einzelnen Benutzer installiert sind (auch als "benutzerspezifische Anwendungen" bezeichnet), werden unsichtbar und können nicht per Remote-Deinstallation entfernt werden, wenn dieser Benutzer nicht angemeldet ist.

Dieses Verhalten unterscheidet sich von Anwendungen, die von mehreren Benutzern auf demselben Gerät verwendet werden (auch als "gerätespezifische Anwendungen" bezeichnet). Gerätespezifische Anwendungen sind für alle Benutzer des Geräts sichtbar und zugänglich.

Aus diesem Grund können benutzerspezifische Anwendungen nur dann deinstalliert werden, wenn der Benutzer angemeldet ist.

Informationsquellen zu installierten Anwendungen

Auf Windows-Geräten ruft der Administrationsagent Informationen über installierte Software aus den folgenden Registrierungsschlüsseln ab:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Enthält Informationen über Anwendungen, die für alle Benutzer installiert sind.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Enthält Informationen über Anwendungen, die für alle Benutzer installiert sind.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Enthält Informationen über Anwendungen, die für den aktuellen Benutzer installiert sind.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Enthält Informationen über Anwendungen, die für bestimmte Benutzer installiert sind.

Ein Windows-Gerät für die Remote-Installation vorbereiten

Die Remote-Installation einer Anwendung auf einem Client-Gerät kann aus den folgenden Gründen fehlerhaft beendet werden:

- Die Aufgabe wurde zuvor schon erfolgreich auf dem Gerät abgeschlossen.

  In diesem Fall muss sie nicht noch einmal ausgeführt werden.

- Beim Aufgabenstart war das Gerät ausgeschaltet.

  In diesem Fall muss das Gerät hochgefahren und die Aufgabe anschließend Neu starten werden.

- Es fehlt eine Verbindung zwischen dem Administrationsserver und dem Administrationsagenten, der auf dem Client-Gerät installiert ist.

  Zur Ursachenforschung können Sie das Tool Remote-Diagnose des Client-Geräts (klactgui) verwenden.

- Wenn der Administrationsagent nicht auf dem Gerät installiert ist, können bei der Remote-Installation des Programms folgende Probleme auftreten:
  - Auf dem Client-Gerät ist Option **Deaktivieren des einfachen Zugriffs auf Dateien** aktiviert.
  - Auf dem Client-Gerät wird der Dienst Server nicht ausgeführt.
  - Auf dem Client-Gerät sind die Ports geschlossen.
  - Die Berechtigungen des Benutzerkontos, unter dem die Aufgabe ausgeführt wird, reichen nicht aus.

  Um Probleme zu vermeiden, die während der Installation der Anwendung auf einem Client-Gerät ohne installierten Administrationsagent auftreten können, müssen Sie vorgehen, wie hier beschrieben: Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center Linux.

Ursprünglich wurde das Tool "riprep" verwendet, um ein Gerät für die Remote-Installation vorzubereiten. Dies Methode zur Konfiguration von Betriebssystemen gilt nun als veraltet. Die Verwendung des riprep-Tools wird für Betriebssysteme, die neuer sind als Windows XP und Windows Server 2003 R2, nicht empfohlen.

Aufgabe zur Remote-Ausführung von Skripten erstellen

Sie können die Aufgabe *Skripte remote ausführen* erstellen, um auf einem Client-Gerät ein Installationspaket auszuführen und eine Anwendung per Fernzugriff zu installieren.

Ein Installationspaket enthält ein zip-Archiv mit einer Reihe von Skripten zur Ausführung auf Client-Geräten sowie die Datei "manifest.json". Weitere Informationen zum Erstellen eines solchen Installationspakets finden Sie in diesem Artikel.

Diese Aufgabe kann nur auf Geräten mit dem Administrationsagenten für Linux gestartet werden.

So starten Sie die Aufgabe Skripte remote ausführen:

1. Gehen Sie zum **Assistent für das Erstellen einer Aufgabe** und wählen Sie den Aufgabentyp **Skripte remote ausführen** aus.
2. Geben Sie den Aufgabennamen ein und wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll. Klicken Sie auf **Weiter**.
3. Wählen Sie ein Installationspaket zur Remote-Ausführung aus, das auf einem zip-Archiv basiert und die Datei "manifest.json" enthält.

   Wenn Sie nicht möchten, dass die Aufgabe auf Geräten, auf denen sie bereits abgeschlossen wurde, erneut ausgeführt wird, aktivieren Sie die Option **Diese Aufgabe nicht auf Geräten ausführen, auf denen sie bereits abgeschlossen wurde**.
4. Wählen Sie ein Benutzerkonto aus, unter dem die Aufgabe ausgeführt wird.

   Wenn Sie das Standardkonto auswählen, wird die Aufgabe vom Administrationsagenten (Root-Benutzerkonto) ausgeführt.

Sobald die Aufgabe *Skripte remote ausführen* gestartet wurde, können Sie das ihr zugewiesene Benutzerkonto nicht mehr ändern. Um das Benutzerkonto für diese Aufgabe zu ändern, beenden Sie die Aufgabe in den Aufgabeneinstellungen und starten Sie sie anschließend mit den korrekten Einstellungen erneut.

5. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

6. Klicken Sie auf **Fertigstellen**.

   Die Aufgabe *Remote-Ausführung von Skripten* wird erstellt und in der Aufgabenliste angezeigt.

Nachdem die Daten von der Aufgabe *Remote-Ausführung von Skripten* empfangen wurden, beschränkt der Administrationsagent den Zugriff auf die abgerufenen Daten für alle Benutzer, mit Ausnahme des Administrators und des in den Aufgabeneinstellungen angegebenen Benutzers.

Installationspaket auf Basis einer Manifestdatei erstellen

So erstellen Sie ein Installationspaket auf Grundlage einer Manifestdatei:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung** → **Installationspakete**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für neue Installationspakete wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.

3. Wählen Sie die Option **Installationspaket auf Basis eines zip-Archivs mit der Datei "manifest.json" für die Aufgabe zur Remote-Ausführung von Skripten erstellen** aus.

4. Geben Sie den Namen des Pakets an und klicken Sie auf **Durchsuchen**.

   Wählen Sie im angezeigten Fenster eine Datei aus, um das Installationspaket zu erstellen.

5. Wählen Sie eine Archivdatei aus, die sich auf einem verfügbaren Datenträger befindet. In diesem Artikel erfahren Sie, wie Sie ein Archiv für diese Aufgabe vorbereiten.

   Die Datei wird auf den Kaspersky Security Center Linux Administrationsserver hochgeladen.

   Das Erstellen des Installationspakets wird gestartet.

   Der Assistent meldet, wenn der Vorgang abgeschlossen ist.

   Falls das Installationspaket nicht erstellt wurde, wird eine entsprechende Meldung angezeigt.

6. Klicken Sie auf die Schaltfläche **Fertigstellen**, um den Assistenten zu schließen.

Das von Ihnen erstellte Installationspaket wird in den Unterordner "Pakete" des Freigegebenen Ordners des Administrationsservers heruntergeladen. Nach dem Herunterladen erscheint das Installationspaket in der Liste der Installationspakete.

Wenn Sie in der Liste der auf dem Administrationsserver verfügbaren Installationspakete auf den Link mit dem Namen eines benutzerdefinierten Installationspakets klicken, haben Sie folgende Optionen:

- Die folgenden Eigenschaften eines Installationspakets anzeigen:
  - **Name.** Der Name des benutzerdefinierten Installationspakets.
  - **Quelle.** Hersteller der Anwendung.
  - **Version.** Version der Anwendung.
  - **Erstellt.** Erstellungsdatum des Installationspakets.
  - **Geändert.** Änderungsdatum des Installationspakets.
  - **Pfad.** Pfad des benutzerdefinierten Installationspakets auf dem Administrationsserver.
- Paketname und Befehlszeilenparameter ändern. Diese Funktion ist nur für Pakete verfügbar, die nicht auf Grundlage von Kaspersky-Anwendungen erstellt wurden.

Archiv für die Aufgabe zur Remote-Ausführung von Skripten vorbereiten

Ein Archiv für die Aufgabe *Skripte remote ausführen* auf Grundlage einer manifest.json-Datei muss die folgenden Anforderungen erfüllen:

- Archivformat: zip.
- Gesamtgröße: maximal 1 GB.
- Die Anzahl der Dateien und Ordner im Archiv ist unbegrenzt.
- Die Manifestdatei des Archivs muss dem unten aufgeführten Schema entsprechen und den Namen "manifest.json" haben. Das Schema wird erst während der Aufgabenausführung auf einem Gerät validiert.

  JSON-Schema der Manifestdatei und Beschreibung der Arrays

  JSON-Schema

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
```

```
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Beispiel für die Manifestdatei

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
```

```
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- Das Archiv muss folgende Struktur besitzen:

  `manifest.json`

  `<file1>`

  `<file2>`

  `<folder1>/<file3>`

  `<folder2>/<folder3>/<file4>`

  `...`

  `<fileX>`

  Die Datei "manifest.json" ist die Manifestdatei für die Aufgabe.

  `<file1>, ...., <fileX>` entspricht den Dateien mit auszuführenden Skripten.

Anwendungen mittels Aufgabe zur Remote-Ausführung von Skripten auf Geräten installieren

Die Aufgabe *Skripte remote ausführen* kann dazu verwendet werden, eine Anwendung auf einem Client-Gerät per Fernzugriff zu installieren. Dazu wird ein benutzerdefiniertes Installationspaket erstellt.

In diesem Artikel erfahren Sie, wie Sie ein Archiv für diese Aufgabe vorbereiten.

Um ein Installationspaket für die Remote-Installation einer Anwendung auf einem Client-Gerät zu erstellen, muss das Archiv, das Sie für diese Aufgabe hochladen möchten, die folgenden Dateien enthalten:

- `<Paketname>.deb`
- **install.sh**

  ```
  sudo apt-get install <Paketname>.deb
  ```

- **manifest.json**

JSON-Schema für die Remote-Installation einer Anwendung

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<bei Bedarf Argumente eingeben>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

Beschreibung der Arrays

1. `version` – Version der Manifestdatei und der Aufgabe.

   Derzeit ist der einzig gültige Wert "1".

2. Die Elemente des Arrays `actions` bestimmen den Aufbau und die Reihenfolge der Skripte, die in der Aufgabe ausgeführt werden.

   Die Ausführungsreihenfolge des Skripts entspricht dem Index (Platz) eines Elements im Array.

3. Für jedes Element des Arrays `actions` sind die folgenden Elemente definiert.

   a. `type` – Typ des ausführbaren Befehls aus Skripten. Derzeit ist der Wert stets `execute`.

   b. `path` – Pfad zur Skriptdatei im Archiv.

   c. `args` – Argumente, die als Teil des ausführbaren Befehls an das Skript übertragen werden.

d. `results` – Array, das abhängig vom Ergebnis der Aufgabe weitere Aktionen definiert.

1. `code` – Wert, den ein Skript zurückgibt.

2. `next` – Aktion, die als nächste ausgeführt werden soll. Die Aktion `continue` führt zur Ausführung des nächsten Skripts (Element im Array `actions`) und die Aktion `break` hält die Aufgabe an.

e. `default_next` – Aktion, wenn ein Skript einen Wert zurückgibt, der nicht in `results` enthalten ist.

Wenn die Aufgabe *Skripte remote ausführen* gestartet wird, lädt der Administrationsagent das Installationspaket mit der Anwendung auf das Client-Gerät hoch. Wenn das Client-Gerät das Installationspaket empfängt, analysiert der Administrationsagent auf diesem Gerät die Datei "manifest.json". Abhängig vom Ergebnis legt der Administrationsagent die Ausführungsreihenfolge der Skripte und Aktionen fest und startet anschließend die Ausführung.

Nach Abschluss der Aufgabe *Skripte remote ausführen* ist die Anwendung auf dem Client-Gerät installiert.

Benachrichtigungen und Überwachung für die Aufgabe zur Remote-Ausführung von Skripten konfigurieren

Für die Aufgabe *Skripte remote ausführen* können Sie die Überwachung, das Verhalten zur Speicherung von Ereignissen und die Benachrichtigungen konfigurieren.

So zeigen Sie den Status der Aufgabe Skripte remote ausführen an:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
   Die Aufgabenliste wird angezeigt.

2. Wählen Sie die Aufgabe aus und klicken Sie auf **Geräteverlauf**.
   Der Aufgabenfortschritt wird angezeigt.

So konfigurieren Sie das Verhalten zur Speicherung von Ereignissen:

1. Klicken Sie in der Aufgabenliste auf die Aufgabe und gehen Sie zur Registerkarte **Einstellungen**.

2. Klicken Sie im Abschnitt **Benachrichtigungen** auf **Einstellungen**.

3. Wählen Sie aus, wie sich die Anwendung nach Abschluss der Aufgabe verhalten soll:

   - **Alle Ereignisse speichern**.
   - **Ereignisse in Bezug auf den Aufgabenfortschritt speichern**.
   - **Nur die Ergebnisse der Aufgabenausführung speichern**.
     Die Ereignisse werden im **Geräteverlauf** und in der **Ereignis-Datenverwaltung** gespeichert.
     Standardmäßig werden nur die Ergebnisse der Aufgabenausführung gespeichert.

Wenn Sie **Alle Ereignisse speichern** auswählen, werden nur die Ergebnisse der Aufgabenausführung gespeichert.

4. Wenn Sie die Ereignisse in der Administrationsserver-Datenbank, im Ereignisprotokoll auf dem Administrationsserver oder auf dem Gerät behalten möchten, aktivieren Sie die entsprechende Option.

Weitere Informationen über die Konfiguration von Benachrichtigungen finden Sie in diesem Artikel.

Lizenzierung

Dieser Abschnitt enthält Informationen:

- Allgemeine Konzepte im Zusammenhang mit der Lizenzierung von Kaspersky Security Center Linux
- Anleitung zur Lizenzverwaltung für verwaltete Kaspersky-Anwendungen

Lizenzierung von Kaspersky Security Center Linux

Dieser Abschnitt beschreibt die grundlegenden Konzepte, die mit der Lizenzierung von Kaspersky Security Center Linux zusammenhängen.

Über den Endbenutzer-Lizenzvertrag

Der *Endbenutzer-Lizenzvertrag* (Lizenzvertrag oder EULA) ist ein rechtsgültiger Vertrag zwischen Ihnen und AO Kaspersky Lab. Er bestimmt die Nutzungsbedingungen für die Anwendung.

Bitte lesen Sie sich den Endbenutzer-Lizenzvertrag sorgfältig durch, bevor Sie die Anwendung nutzen.

Kaspersky Security Center Linux und die einzelnen Komponenten (z. B. Administrationsagent) haben jeweils eine eigene EULA.

Sie können die Bedingungen des Endbenutzer-Lizenzvertrags für Kaspersky Security Center Linux wie folgt anzeigen:

- Während der Installation von Kaspersky Security Center.
- Mithilfe des Dokuments license.txt, das zum Lieferumfang von Kaspersky Security Center gehört.
- Mithilfe des Dokuments license.txt im Installationsordner von Kaspersky Security Center.
- Durch Herunterladen der Datei license.txt von der Website von Kaspersky.

Sie können die Bedingungen des Endbenutzer-Lizenzvertrags für den Administrationsagenten für Linux wie folgt anzeigen:

- Während das Distributionspaket für den Administrationsagenten von den Kaspersky-Webservern heruntergeladen wird.
- Während der Installation des Administrationsagenten für Linux.
- Im Dokument license.txt, das im Distributionspaket des Administrationsagenten für Linux enthalten ist.

- Im Dokument license.txt, das sich im Installationsordner des Administrationsagenten für Linux befindet.
- Durch Herunterladen der Datei license.txt von der Website von Kaspersky.

Wenn Sie bei der Anwendungsinstallation dem Text des Endbenutzer-Lizenzvertrags zustimmen, gelten die Bedingungen des Endbenutzer-Lizenzvertrags als akzeptiert. Falls Sie den Lizenzvertrag ablehnen, brechen Sie die Anwendungsinstallation ab und nutzen Sie die Anwendung nicht.

Über die Lizenz

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für Kaspersky Security Center Linux, das Ihnen gemäß den Bedingungen des unterzeichneten Lizenzvertrags (Endbenutzer-Lizenzvertrag) überlassen wird.

Der Umfang der Leistungen und die Laufzeit hängen vom Typ der Lizenz ab, mit der die Anwendung verwendet wird.

Es sind folgende Lizenztypen vorgesehen:

- *Test*

  Eine kostenlose Lizenz zum Kennenlernen der Anwendung. Eine Demolizenz verfügt in der Regel über eine kurze Gültigkeitsdauer.

  Nachdem die Gültigkeit einer Demolizenz abgelaufen ist, stellt Kaspersky Security Center Linux die Funktion ein. Um die Anwendung weiter nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.

  Die Anwendung kann nur einmal im Rahmen einer Demolizenz verwendet werden.

- *Kommerziell*

  Eine kostenpflichtige Lizenz.

  Wenn eine kommerzielle Lizenz abläuft, werden wichtige Anwendungsfunktionen deaktiviert. Zur weiteren Nutzung von Kaspersky Security Center ist eine Verlängerung der kommerziellen Lizenz erforderlich. Nach Ablauf einer kommerziellen Lizenz können Sie die Anwendung nicht mehr verwenden und müssen es von Ihrem Gerät entfernen.

  Es wird empfohlen, die Gültigkeitsdauer Ihrer Lizenz vor deren Ablaufdatum zu verlängern, um einen ununterbrochenen Schutz vor allen Sicherheitsbedrohungen zu gewährleisten.

Über das Lizenzzertifikat

Ein *Lizenzzertifikat* ist ein Dokument, das Ihnen zusammen mit einer Schlüsseldatei bzw. einem Aktivierungscode übergeben wird.

Das Lizenzzertifikat enthält folgende Informationen über die ausgestellte Lizenz:

- Lizenz-ID oder Bestellnummer
- Informationen über den Benutzer, dem die Lizenz ausgestellt wird
- Informationen über die Anwendung, das mit der ausgestellten Lizenz aktiviert werden kann
- Maximale Anzahl von Lizenzeinheiten (z. B. Geräte, auf denen die Anwendung unter dieser Lizenz verwendet werden kann)

- Datum für den Beginn der Lizenzgültigkeit
- Ablaufdatum der Lizenz oder Gültigkeitsdauer der Lizenz
- Lizenztyp

Über den Lizenzschlüssel

Ein *Lizenzschlüssel* ist eine Bitsequenz, mit deren Hilfe Sie die Anwendung aktivieren können, um diese dann in Übereinstimmung mit dem Endbenutzer-Lizenzvertrag zu nutzen. Der Lizenzschlüssel wird von den Experten von Kaspersky generiert.

Sie können einen Lizenzschlüssel mithilfe einer der folgenden Methoden zur Anwendung hinzufügen: durch Anwendung einer *Schlüsseldatei* oder Eingabe eines *Aktivierungscodes*. Nachdem Sie den Lizenzschlüssel in der Anwendung hinzugefügt haben, wird er in der Programmoberfläche als eindeutige Folge aus Buchstaben und Ziffern angezeigt.

Ein Lizenzschlüssel kann von Kaspersky gesperrt werden, falls die Bedingungen des Lizenzvertrags verletzt wurden. Wenn ein Lizenzschlüssel gesperrt wurde, muss ein anderer Schlüssel hinzugefügt werden, um die Anwendung zu nutzen.

Ein Lizenzschlüssel kann entweder aktiv oder zusätzlich (Reserve) sein.

Ein *aktiver Lizenzschlüssel* ist ein Lizenzschlüssel, der momentan von der Anwendung verwendet wird. Ein aktiver Lizenzschlüssel kann für eine Test- oder kommerzielle Lizenz hinzugefügt werden. In der Anwendung kann jeweils nur ein aktiver Lizenzschlüssel vorhanden sein.

Ein *zusätzlicher (oder Reserve-) Lizenzschlüssel* ist ein Lizenzschlüssel, der das Recht auf Nutzung der Anwendung bestätigt, jedoch im Augenblick nicht verwendet wird. Der Reserve-Lizenzschlüssel wird automatisch aktiviert, wenn die Gültigkeitsdauer der Lizenz abläuft, die zum aktiven Lizenzschlüssel gehört. Ein Reserve-Lizenzschlüssel kann nur hinzugefügt werden, wenn ein aktiver Lizenzschlüssel vorhanden ist.

Der Lizenzschlüssel für eine Demolizenz kann als aktiver Lizenzschlüssel hinzugefügt werden. Der Lizenzschlüssel für eine Demolizenz kann nicht als Reserve-Lizenzschlüssel hinzugefügt werden.

Anzeigen der Datenschutzrichtlinie

Die Datenschutzrichtlinie ist online verfügbar unter https://www.kaspersky.de/products-and-services-privacy-policy.

Die Datenschutzrichtlinie ist auch offline verfügbar:

- Sie können die Datenschutzrichtlinie lesen, bevor Sie Kaspersky Security Center Linux installieren.
- Der Text der Datenschutzrichtlinie ist in der Datei license.txt im Installationsordner von Kaspersky Security Center Linux enthalten.
- Die Datei privacy_policy.txt ist auf einem verwalteten Gerät im Installationsordner des Administrationsagenten verfügbar.
- Sie können die Datei privacy_policy.txt aus dem Distributionspaket des Administrationsagenten entpacken.

Varianten der Lizenzierung von Kaspersky Security Center

Kaspersky Security Center besitzt folgende Ausführungsmodi:

- **Basisfunktionen der Verwaltungskonsole**

  Kaspersky Security Center arbeitet in diesem Modus, bevor die Anwendung aktiviert wird oder nachdem die kommerzielle Lizenz abläuft. Die Anwendung Kaspersky Security Center, welche die Basisfunktionen der Verwaltungskonsole unterstützt, wird zusammen mit den Kaspersky-Produkten geliefert, die für den Schutz des Unternehmensnetzwerks konzipiert sind. Außerdem steht es auf der Website von Kaspersky zum Download bereit.

- **Kommerzielle Lizenz**

  Wenn Sie zusätzliche Funktionen benötigen, die nicht zu den Grundfunktionen der Verwaltungskonsole gehören, müssen Sie eine kommerzielle Lizenz erwerben.

  Stellen Sie beim Hinzufügen eines Lizenzschlüssels im Eigenschaftenfenster des Administrationsservers sicher, dass Sie den Lizenzschlüssel hinzufügen, mit dem sich Kaspersky Security Center Linux verwenden lässt. Sie können diese Informationen auf der Kaspersky-Website finden. Die Websites der einzelnen Lösungen bieten eine Liste der Anwendungen, die in der jeweiligen Lösung enthalten sind. Der Administrationsserver akzeptiert möglicherweise nicht unterstützte Lizenzschlüssel, beispielsweise Lizenzschlüssel für Kaspersky Endpoint Security Cloud, aber diese Lizenzschlüssel bieten neben den grundlegenden Funktionen der Verwaltungskonsole keine neuen Funktionen.

Funktion oder Eigenschaft	Ausführungsmodus von Kaspersky Security Center Linux	
	Keine Lizenz	Kommerzielle Lizenz
Basisfunktionen der Verwaltungskonsole Es stehen folgende Funktionen zur Verfügung: • Virtuelle Administrationsserver erstellen, um ein Netzwerk entfernter Standorte bzw. Kundenunternehmen zu verwalten • Hierarchie der Administrationsgruppen erstellen, um eine Reihe von Geräten als Ganzes zu verwalten • Remote-Installation von Anwendungen • Einstellungen der auf den Client-Geräten installierten Anwendungen zentral anpassen • Status der Antiviren-Sicherheit eines Unternehmens kontrollieren • Benutzerrollen verwalten • Statistiken und Berichte über die Ausführung von Anwendungen sowie Benachrichtigungen über kritische Ereignisse erhalten • Zentral Dateien verwalten, die in die Quarantäne, ins Backup oder in die Ablage für Dateien mit verschobener Verarbeitung verschoben wurden • Verschlüsselung und Datenschutz verwalten • Liste der durch eine Netzwerkabfrage gefundenen Geräte anzeigen und manuell bearbeiten • Liste der Betriebssystem-Abbilder anzeigen, die für die Remote-Installation verfügbar sind	✓	✓

Funktion oder Eigenschaft	Ausführungsmodus von Kaspersky Security Center Linux	
	Keine Lizenz	Kommerzielle Lizenz
Schwachstellen- und Patch-Management: Basisfunktionen Für die folgenden Aufgaben ist keine kommerzielle Lizenz erforderlich: • Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* Über die Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates erhält Kaspersky Security Center Linux eine Liste der erkannten Schwachstellen und der erforderlichen Updates für Drittanbieter-Programme, die auf den verwalteten Geräten installiert ist. • Aufgabe *Schwachstellen schließen* Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für Software von Microsoft und individuelle Korrekturen für Drittanbieter-Programme. Um die Aufgabe zu verwenden, müssen Sie manuell individuelle Korrekturen angeben.	✓	✓
Schwachstellen- und Patch-Management: Erweiterte Funktionen Sie können Regeln für die automatische Remote-Installation von Programm-Updates und das automatische Schließen von Schwachstellen festlegen.	—	✓
Systemverwaltung Es stehen folgende Funktionen zur Verfügung: • Remote-Berechtigung für die Verbindung zu Client-Geräten durch eine Komponente von Microsoft® Windows® namens Remote Desktop Connection • Remote-Verbindung mit Client-Geräten über Windows Desktopfreigabe	—	✓
Exportieren von Ereignissen mittels Syslog-Protokoll in SIEM-Systeme. Gemäß dem Protokoll Syslog können beliebige Ereignisse, die auf dem Kaspersky Security Center Administrationsserver und in den auf den verwalteten Geräten installierten Kaspersky-Anwendungen auftreten, übertragen werden. Das Syslog-Protokoll ist ein Standardprotokoll für das Aufzeichnen von Nachrichten. Sie können es für den Export von Ereignissen ein beliebiges SIEM-System verwenden.	✓	✓
Aggregation von Alarmen und Ausführen von Reaktionsmaßnahmen über Active Directory, KASAP und Kaspersky TIP Sandbox	—	✓

Über die Schlüsseldatei

Eine *Schlüsseldatei* ist eine Datei mit der Erweiterung key, die Sie von Kaspersky erhalten. Schlüsseldateien dienen zum Aktivieren der Anwendung durch Hinzufügen eines Lizenzschlüssels.

Sie erhalten eine Schlüsseldatei an die E-Mail-Adresse, die Sie beim Kauf von Kaspersky Security Center oder bei der Anforderung der Testversion von Kaspersky Security Center angegeben haben.

Um die Anwendung mithilfe der Schlüsseldatei zu aktivieren, ist keine Verbindung mit den Kaspersky-Aktivierungsservern erforderlich.

Wenn die Schlüsseldatei versehentlich gelöscht wurde, können Sie diese wiederherstellen. Eine Schlüsseldatei kann beispielsweise für die Registrierung eines Kaspersky CompanyAccount erforderlich sein.

Um Ihre Schlüsseldatei wiederherzustellen, führen Sie eine der folgenden Aktionen aus:

- Wenden Sie sich an den Lizenzverkäufer.
- Schlüsseldatei anhand eines vorhandenen Aktivierungscodes auf der Website von Kaspersky abrufen.

Über die Bereitstellung von Daten

An Dritte übertragene Daten

Wenn Sie die Funktion "Verwaltung mobiler Geräte" verwenden, wird der Cloud-Messaging-Dienst Google Firebase verwendet, um Befehle mittels Push-Benachrichtigungen rechtzeitig an Geräte zu senden, auf denen das Android-Betriebssystem ausgeführt wird. Wenn ein Benutzer die Verwendung des Google Firebase Cloud Messaging-Dienstes konfiguriert hat, erklärt sich der Benutzer damit einverstanden, die folgenden Informationen im automatischen Modus dem Google Firebase Cloud Messaging-Dienst zur Verfügung zu stellen:

- Instanz-ID
- Software-ID des Google Firebase Cloud Messaging-Dienstes
- Version der installierten Software
- Die vollständige Versionsnummer der Software
- Version von Google Play
- Name des Programmpakets der Software
- Versions des Schemas für die bereitgestellten Daten
- Version des Betriebssystems
- Software-ID

Um den Informationsaustausch mit dem Google Firebase Cloud-Messaging-Dienst zu blockieren, muss der Benutzer die Einstellungen des Google Firebase Cloud-Messaging-Dienstes zurücksetzen.

Wenn Sie Funktion "Verwaltung mobiler Geräte" verwenden, wird der Apple Push Notification Service (APNS) verwendet, um Befehle rechtzeitig mittels Push-Benachrichtigungen an Geräte zu übermitteln, auf denen ein iOS-Betriebssystem ausgeführt wird. Wenn der Benutzer ein APNs-Zertifikat auf einem iOS MDM-Server installiert hat, ein iOS MDM-Profil mit einer Reihe von Einstellungen für die Verbindung von mobilen iOS-Geräten mit der Software erstellt, und wenn er dieses iOS MDM-Profil auf mobilen Geräten installiert, erklärt er sich damit einverstanden, die folgenden Informationen an APNs im automatischen Modus bereitzustellen:

- Token – Push-Token des Geräts. Der Server verwendet diesen Token beim Senden von Push-Benachrichtigungen an das Gerät.
- PushMagic – Zeichenfolge, die in der Push-Benachrichtigung enthalten sein muss. Der Wert dieser Zeichenfolge wird vom Gerät generiert.

An AO Kaspersky Lab übertragene Daten

Wenn dem Benutzer die Funktionen von Kaspersky Extended Detection and Response Optimum zur Verfügung stehen, überträgt Kaspersky Security Center Linux in den folgenden Fällen Daten:

- Um einem Mitarbeiter eine Schulung zuzuweisen, überträgt Kaspersky Security Center Linux die folgenden Daten an die Kaspersky Automated Security Awareness Platform (KASAP): E-Mail-Adresse des Benutzers, alternative E-Mail-Adresse des Benutzers (falls vorhanden), Benutzer-ID in KASAP und ID der Schulungsgruppe.

- Um mittels des Dienstes "Kaspersky Cloud Sandbox" schädliches Verhalten auszuführen und zu erkennen, überträgt die verwaltete Kaspersky-Anwendung Objekte, die sich in Quarantäne befinden, und Dateien, die während der Ausführung der übertragenen Objekte erstellt wurden, vom Administrationsserver über den Administrationsagenten und anschließend über die Kaspersky Security Center Web Console an den Dienst "Kaspersky Cloud Sandbox".

Lokal verarbeitete Daten

Kaspersky Security Center Linux dient dazu, die wichtigsten Aufgaben zur Verwaltung und Wartung des Antiviren-Schutzes in einem Unternehmensnetzwerk zentral zu erledigen. Kaspersky Security Center Linux ermöglicht es einem Administrator, auf detaillierte Informationen über die Sicherheitsstufe des Unternehmensnetzwerks zuzugreifen. Mit Kaspersky Security Center Linux kann ein Administrator alle Schutzkomponenten konfigurieren, die auf Kaspersky-Anwendungen basieren. Die folgenden Hauptfunktionen werden von Kaspersky Security Center Linux ausgeführt:

- Erkennen von Geräten und deren Benutzern im Unternehmensnetzwerk
- Erstellen einer Hierarchie von Administrierungsgruppen für die Geräteverwaltung
- Installieren von Kaspersky-Anwendungen auf Geräten
- Verwalten der Einstellungen und Aufgaben von installierten Programmen
- Verwalten der Updates für Kaspersky- und Drittanbieter-Anwendungen sowie Auffinden und Schließen von Schwachstellen
- Aktivieren von Kaspersky-Anwendungen auf Geräten
- Verwalten von Benutzerkonten
- Anzeigen von Informationen zur Ausführung von Kaspersky-Anwendungen auf Geräten
- Anzeigen von Berichten
- Aktivieren der Integration mit Kaspersky-Diensten

Um seine Hauptfunktionen auszuführen, kann Kaspersky Security Center Linux die folgenden Informationen empfangen, speichern und verarbeiten:

- Informationen über die Geräte im Unternehmensnetzwerk, die durch das Abfragen von Domänencontrollern (Active Directory, Samba, FreeIPA und ALD Pro) oder durch das Abfragen von IP-Intervallen abgerufen wurden. Der Administrationsserver ruft unabhängig Daten ab oder empfängt Daten vom Administrationsagent.

- Informationen von Domänencontrollern (Active Directory, Samba, FreeIPA und ALD Pro) zu Organisationseinheiten, Domänen, Benutzer und Benutzergruppen. Der Administrationsserver bezieht die Daten entweder selbst oder erhält sie von einem Administrationsagenten, der als Verteilungspunkt fungiert.

- Einzelheiten zu den verwalteten Geräten Der Administrationsagent übermittelt die unten aufgeführten Daten von dem Gerät an den Administrationsserver. Der Benutzer gibt den Anzeigenamen und die Beschreibung des Gerätes auf der Benutzeroberfläche von Kaspersky Security Center Web Console ein:

    - Technische Spezifikationen des verwalteten Geräts und seiner Komponenten, die zur Geräteidentifizierung erforderlich sind: Anzeigename und Beschreibung des Geräts, Typ und Name der Windows-Domäne (für Geräte, die zu einer Windows-Domäne gehören), Gerätename in der Windows-Umgebung (für Geräte, die zu einer Windows-Domäne gehören), DNS-Domäne und DNS-Name, IPv4-Adresse, IPv6-Adresse, Netzwerkadresse, MAC-Adresse, Seriennummer, Betriebssystemtyp, ob das Gerät eine virtuelle Maschine mit Hypervisor-Typ ist oder ob das Gerät eine dynamische virtuelle Maschine als Teil von VDI ist.

    - Andere Spezifikationen der verwalteten Geräte und ihrer Komponenten, die für die Überprüfung der verwalteten Geräte und zur Entscheidung über zu installierende Patches und Updates erforderlich sind: Betriebssystemarchitektur, Betriebssystemhersteller, Build-Nummer des Betriebssystems, Release-ID des Betriebssystems, Ordner des Speicherorts des Betriebssystems, wenn es sich bei dem Gerät um eine virtuelle Maschine handelt – der Typ der virtuellen Maschine, Name des das Gerät verwaltenden Administrationsservers.

    - Details zu Aktionen auf verwalteten Geräten: Datum und Uhrzeit des letzten Updates; Uhrzeit, zu der das Gerät zuletzt im Netzwerk sichtbar war; Neustart-Wartestatus; Uhrzeit, zu der das Gerät eingeschaltet wurde.

    - Details zu Gerätebenutzerkonten und den deren Arbeitssitzungen.

- Daten, die beim Ausführen der Ferndiagnose auf einem verwalteten Gerät empfangen werden: Ablaufverfolgungsdateien, Systeminformationen, Details zu den auf dem Gerät installierten Kaspersky-Anwendungen, Dump-Dateien, Ereignisprotokolle, Ausführungsergebnisse der vom Kaspersky Technischen Support bereitgestellten Diagnoseskripte.

- Statistiken zum Verteilungspunkt-Betrieb, wenn das Gerät ein Verteilungspunkt ist. Der Administrationsagent übermittelt Daten von dem Gerät an den Administrationsserver.

- Vom Benutzer in Kaspersky Security Center Web Console eingegebene Einstellungen für die Verteilungspunkte.

- Daten, die für die Verbindung von mobilen Geräten mir dem Administrationsserver notwendig sind: Zertifikat, Port der mobilen Verbindung, Verbindungsadresse des Administrationsservers. Der Benutzer gibt die Daten in die Kaspersky Security Center Web Console ein.

- Details zu mobilen Geräten, die mithilfe des mobilen Protokolls übertragen werden. Die unten aufgelisteten Daten werden vom mobilen Gerät an den Administrationsserver übertragen:

    - Informationen über die Anwendung: Name und vollständige Versionsnummer der Anwendung, Datum und Uhrzeit der Anwendungsinstallation, Status des Echtzeitschutzes auf dem Gerät, Sitzungs-ID.

    - Informationen über die von der Anwendung verwendeten Lizenzschlüssel: Seriennummer und Lizenztyp des Lizenzschlüssels, Status des Lizenzschlüssels, Gültigkeitsdauer des Lizenzschlüssels in Tagen, Datum von Erstellung und Ablauf des Lizenzschlüssels, Name des Unternehmens, für das die Lizenz bereitgestellt wurde, zusätzliche Informationen im Falle eines Abonnements (Flag des Abonnements, Ablaufdatum und Anzahl an verfügbaren Tagen zur Verlängerung des Abonnements, Webadresse des Abonnementanbieters, aktueller Status des Abonnements und Grund für den Erhalt dieses Status), Datum und Uhrzeit der Anwendungsaktivierung auf dem Gerät, Datum und Uhrzeit des Ablaufs der Lizenz auf dem Gerät.

- Informationen über das verwaltete Gerät: Gerätename, Geräte-ID, Gerätetyp, IMEI des Geräts (sofern verfügbar), Seriennummer des Geräts (sofern verfügbar), Gerätehersteller, Name der CPU-Familie des Geräts, Fingerabdruck des Zertifikats des Gerätebesitzers, Typ des Betriebssystems, Version des Betriebssystems, Betriebssystem Name, gesamter Speicherplatz auf dem Gerät, Name des Servers, dem das Gerät angehört, IP-Adresse des Geräts, Name der Gerätegruppe, eindeutiger Name des Benutzers, eindeutiger Name der Domäne, Einmalkennwort oder Domänenkennwort.

- Informationen über das Ausführungsergebnis benutzerdefinierter Befehle: ID des Befehls, Status der Befehlsausführung, Ergebnis der Befehlsausführung; für den Befehl zum Orten des Geräts: Breitengrad, Längengrad, Höhe und Bewegungsgeschwindigkeit des Geräts; für den Befehl zum Aufnehmen eines Fahndungsfotos: Fotos, die von der Frontkamera des mobilen Geräts beim Entsperren des Mobilgeräts aufgenommen wurden.

- Informationen zur Untersuchung des Geräts: Datum und Uhrzeit der letzten Untersuchung des Geräts; vollständiger Pfad im Dateisystem, von dem aus die Untersuchung gestartet wurde; Anzahl der untersuchten Objekte; Anzahl der gefundenen schädlichen Objekte; Anzahl der gesperrten, gelöschten und desinfizierten Objekte; Anzahl der Objekte, die nicht desinfiziert werden konnten; Anzahl der Validierungsfehler; Anzahl der beendeten Prozesse.

- Informationen über die Ausführung der Komponenten der Anwendung und der einzelnen Aufgaben, dargestellt als Ereignisse:

    - Event ID.

    - Ereigniskategorie.

    - Name und Typ des Ereignisses.

    - Beschreibung der Ereignisursache.

    - Datum und Zeitpunkt des aufgetretenen Ereignisses.

    - Informationen über die Ereignisse des Diebstahlschutzes (Code zur Entsperrung des Geräts, Gerätekoordinaten, Methode der Befehlsübermittlung, Liste der gelöschten Daten).

    - Ergebnisse der Verarbeitung eines gefundenen Objekts oder einer Aktion (Name der Datei auf dem Gerät; Name der Anwendung; Name der Bedrohung; Bedrohungstyp; Art der mit der Datei durchgeführten Aktion; Ergebnis der Aktion; Fehlercode, falls aufgetreten).

    - Informationen über die ausgelöste Übereinstimmungsregel (Kriterium der Regel; angewendete Aktion; Beschreibung des Fehlers bei der Anwendung der Aktion, falls aufgetreten).

    - Informationen über den Fehler bei der Ausführung der Anwendung (Version der Anwendung, Version des Betriebssystems, Name des Geräts, Fehlerbeschreibung).

    - Informationen über den Fehler von Samsung KNOX (Fehlercode und URL, von der die Datei nicht heruntergeladen werden konnte).

    - Informationen über die Berechtigungen, die der Anwendung gewährt wurden.

    - Informationen zu allen auf dem verwalteten Gerät installierten Anwendungen (Name der Anwendung, Installationsstatus).

        - Informationen über das weltweite Akzeptieren des Endbenutzer-Lizenzvertrags (EULA): EULA-ID, EULA-Zeitstempel, EULA-Text.

        - Einstellungen von Google Firebase Cloud Messaging: ID des Absenders, ID der Geräteregistrierung.

    - Informationen über die öffentliche IP-Adresse des Geräts.

- Details zu mobilen Geräten, die mit dem iOS MDM-Protokoll übertragen werden. Die unten aufgelisteten Daten werden vom mobilen Gerät an den Administrationsserver übertragen:

    - Technische Spezifikationen des mobilen Geräts und seiner Komponenten, die zur Geräteidentifizierung erforderlich sind: Gerätename, Modell, Name, Version und Build-Nummer des Betriebssystems, Gerätemodellnummer, IMEI-Nummer, Telefonnummer, UDID, MEID, Seriennummer, Größe des belegten und verfügbaren Speichers, Modem-Firmware-Version, Bluetooth-MAC-Adresse, Wi-Fi-MAC-Adresse und SIM-Karten-Details (ICCID als Teil der SIM-Karten-ID).

    - Details des vom verwalteten Gerät verwendeten Mobilfunknetzes: Mobilfunknetztyp, Name des derzeit verwendeten Mobilfunknetzes, Name des Heim-Mobilfunknetzes, Version der Mobilfunknetzbetreibereinstellungen, Sprach-Roaming- und Daten-Roaming-Status, Ländercode des Mobilfunknetzes Heimnetzwerk, Ländercode des Wohnsitzes, Code des aktuell verwendeten Netzwerks und Verschlüsselungsgrad.

    - Sicherheitseinstellungen des mobilen Geräts: Verwendung eines Kennworts und dessen Übereinstimmung mit den Richtlinieneinstellungen, Liste der installierten Zertifikate, Apps und Konfigurationsprofile.

    - Datum und Uhrzeit der letzten Synchronisation mit dem Administrationsserver und Status der Geräteverwaltung.

- Details zu den über das WebRTC-Protokoll übertragenen Mobilgerätedaten: Bildschirmfoto des Geräts.

- Details zu Dateien, die zur Übertragung an mobile Geräte angegeben sind. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Einzelheiten zu den auf dem Gerät installierten Kaspersky-Anwendungen. Die verwaltete Anwendung überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver:

    - Einstellungen der auf dem verwalteten Gerät installierten Kaspersky-Anwendungen: Name und Version der Kaspersky-Anwendung, Status, Echtzeitschutzstatus, Datum und Uhrzeit der letzten Untersuchung des Geräts, Anzahl der erkannten Bedrohungen, Anzahl der Objekte, deren Desinfektion fehlgeschlagen ist, Verfügbarkeit und Status der Anwendungskomponenten, Details zu den Einstellungen und Aufgaben von Kaspersky-Anwendungen, Informationen zu aktiven und Reserve-Lizenzschlüsseln, Installationsdatum der Anwendung und ID.

    - Statistiken zur Anwendungsoperation: Ereignisse im Zusammenhang mit Statusveränderungen von Komponenten der Kaspersky-Anwendungen auf dem verwalteten Gerät und im Zusammenhang mit der Ausführung von Aufgaben, die von den Softwarekomponenten ausgelöst werden.

    - Der Status des Geräts wird von der Kaspersky-Anwendung bestimmt.

    - Von der Kaspersky-Anwendung zugewiesene Tags.

- Daten, die in Ereignissen der Komponenten von Kaspersky Security Center Linux und der durch Kaspersky verwalteten Anwendungen enthalten sind. Der Administrationsagent übermittelt Daten von dem Gerät an den Administrationsserver.

- Daten, die zur Integration von Kaspersky Security Center Linux in ein SIEM-System für den Ereignisexport erforderlich sind. Der Benutzer gibt die Daten in die Kaspersky Security Center Web Console ein.

- Daten, die für die Integration von Kaspersky Security Center Linux mit Domänencontrollern (Active Directory, Samba, FreeIPA und ALD Pro) erforderlich sind. Der Benutzer gibt die Daten in die Kaspersky Security Center Web Console ein.
- Keytab-Dateien zum Verbinden mit Kerberos Single Sign-On. Der Benutzer gibt die Daten in die Kaspersky Security Center Web Console ein.
- Daten, die zum Konfigurieren der Verbindung zum Proxyserver für die Internetverbindung erforderlich sind. Der Benutzer gibt die Daten in die Kaspersky Security Center Web Console ein.
- Einstellungen der Komponenten von Kaspersky Security Center Linux und der durch Kaspersky verwalteten Anwendungen in Richtlinien und Richtlinienprofilen. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.
- Aufgabeneinstellungen der Komponenten von Kaspersky Security Center Linux und der durch Kaspersky verwalteten Anwendungen. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.
- Daten, die von der Funktion zur Systemverwaltung verarbeitetet werden. Der Administrationsagent überträgt die folgenden Informationen vom Gerät an den Administrationsserver:
  - Informationen über erkannte Hardware auf verwalteten Geräten (Hardware-Register).

    Wenn der Administrationsagent auf einem Windows-Gerät installiert ist, sendet er nur die folgenden Informationen über die Gerätehardware an den Administrationsserver:

    - Arbeitsspeicher
    - Massenspeichergeräte
    - Mainboard
    - Prozessor
    - Netzwerkadapter
    - Monitore
    - Grafikkarte
    - Soundkarte

    Wenn der Administrationsagent auf einem Linux- oder macOS-Gerät installiert ist, sendet er die folgenden Informationen über die Gerätehardware an den Administrationsserver (vorausgesetzt, diese Information wird durch das Betriebssystem bereitgestellt):

    - Gesamtgröße des Arbeitsspeichers
    - Gesamtgröße der Massenspeicher
    - Mainboard
    - Prozessor
    - Netzwerkadapter

- Einzelheiten zu auf verwalteten Geräten installierten Anwendungen und Patches (Programm-Registry). Die Anwendung kann mit den Informationen über die ausführbaren Dateien verglichen werden, die von der Funktion "Programmkontrolle" auf den Geräten erkannt wurden.

- Details über Schwachstellen in Drittanbieter-Programmen, die auf verwalteten Geräten gefunden wurden.

- Details über verfügbare Updates für Drittanbieter-Anwendungen, die auf verwalteten Geräten installiert sind.

- Erforderliche Daten zum Herunterladen von Updates auf einen isolierten Administrationsserver, um Schwachstellen in Drittanbieter-Programmen auf verwalteten Geräten zu schließen. Mittels des Administrationsservers-Tools "klscflag" gibt der Benutzer Daten ein und überträgt diese.

- Benutzerkategorien der Anwendungen. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Informationen über ausführbaren Dateien, die auf verwalteten Geräten durch die Komponente "Programmkontrolle" gefunden werden. Die verwaltete Anwendung überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien der entsprechenden Anwendung.

- Details zu Dateien, die ins Backup verschoben wurden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Details zu Dateien, die in die Quarantäne verschoben wurden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Informationen zu Dateien, die von Kaspersky-Spezialisten für eine detaillierte Analyse angefordert wurden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Details zum Status und Auslösen von Regeln zur Adaptiven Kontrolle von Anomalien. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Informationen über externe Geräte (Speichereinheiten, Tools zum Informationstransfer, Hardcopy-Tools und Verbindungsbusse), die auf dem verwalteten Gerät installiert oder damit verbunden sind und von der Gerätekontrolle erkannt werden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien der entsprechenden Anwendung.

- Informationen über verschlüsselte Windows-basierte Geräte und den Verschlüsselungsstatus. Eine verwaltete Anwendung überträgt die Daten von dem Gerät über den Administrationsagenten an den Administrationsserver.

- Informationen über Fehler bei der Verschlüsselung von Daten auf den Geräten. Die Verschlüsselung wird von der Funktion zur Datenverschlüsselung der Kaspersky-Anwendungen durchgeführt. Ein verwaltetes Programm überträgt die Daten von dem Gerät über den Administrationsagenten an den Administrationsserver. Eine vollständige Liste der Daten finden Sie in der Online-Hilfe des entsprechenden Anwendungen.

- Liste der verwalteten speicherprogrammierbaren Steuerungen (SPS). Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Daten, die zur Erstellung einer Übersicht über die Ausbreitung einer Bedrohung benötigt werden. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien der entsprechenden Anwendung.

- Informationen über Versuche von Unternehmensmitarbeitern, auf Cloud-Dienste zuzugreifen. Die verwaltete Anwendung überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver. Eine vollständige Liste der Daten finden Sie in den Hilfedateien des entsprechenden Programms.

- Daten, die für die Integration von Kaspersky Security Center in Dienst von Kaspersky Managed Detection and Response erforderlich sind (das dedizierte Plug-In muss für Kaspersky Security Center Web Console installiert sein): Token der Initiierung der Integration, Token der Integration und Token der Benutzersitzung. Der Benutzer gibt den Token für die Initiierung der Integration in die Benutzeroberfläche der Kaspersky Security Center Web Console ein. Der Kaspersky MDR-Dienst überträgt die Token für die Integration und für die Benutzersitzung über das dedizierte Plug-In.

- Daten, die zur Integration von Kaspersky Security Center Linux mit Kaspersky Cloud Sandbox und dem Kaspersky Threat Intelligence Portal erforderlich sind (erfordert die Installation des entsprechenden Plug-ins für die Kaspersky Security Center Web Console): ein Token zur Integration und ein Token für die Autorisierung. Der Benutzer gibt einen Token zur Integration in die Oberfläche der Kaspersky Security Center Web Console ein. Die Kaspersky Security Center Web Console überträgt einen Token für die Autorisierung in einer Anfrage an die API von Kaspersky Cloud Sandbox.

- Daten, die zur Integration von Kaspersky Security Center Linux mit dem Dienst der Kaspersky Automated Security Awareness Platform (KASAP) erforderlich sind: API-Token für den Zugriff auf die KASAP Open API und eine URL (ein Link für den Zugriff auf KASAP über Open API).

- Details der eingegebenen Aktivierungscodes und Schlüsseldateien. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Benutzerkonten: Name, Beschreibung, vollständiger Name, E-Mail-Adresse, Haupttelefonnummer, Kennwort, vom Administrationsserver generierter geheimer Schlüssel und Einmalkennwort für die Zwei-Faktor-Authentifizierung. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Revisionsverlauf von verwalteten Objekten. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- IP-Adresse des Geräts, auf dem eine Revision von einem Benutzer erstellt wurde. Die IP-Adresse wird vom Administrationsserver automatisch festgelegt.

- Register der gelöschten Managementobjekte. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Aus der Datei erzeugte Installationspakete wie auch Installationseinstellungen. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Daten, die für die Anzeige für Neuigkeiten von Kaspersky in der Kaspersky Security Center Web Console erforderlich sind. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Daten, die für das Funktionieren von Plug-Ins verwalteter Anwendungen in Kaspersky Security Center Web Console erforderlich sind und die von den Plug-Ins in der Administrationsserver-Datenbank während ihres Regelbetriebs gespeichert werden. Die Beschreibung und Möglichkeiten zur Bereitstellung der Daten finden Sie in den Hilfedateien der entsprechenden Anwendung.

- Benutzereinstellungen für Kaspersky Security Center Web Console: Sprache und Schema der Benutzeroberfläche, Einstellungen für die Anzeige des Überwachungsfensters, Status der Benachrichtigungen (bereits gelesen / noch nicht gelesen), Status der Spalten in Tabellen (Eingeblendet / Ausgeblendet), Fortschritt des Trainingsmodus. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Zertifikat für eine sichere Verbindung verwalteter Geräte mit den Komponenten von Kaspersky Security Center Linux. Mittels des Administrationsservers-Tools "klsetsrvcert" gibt der Benutzer Daten ein und überträgt diese.

- Zertifikate zum Herstellen einer Vertrauensstellung für die internen Webressourcen des Unternehmens. Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Informationen darüber, welche Bedingungen der rechtlichen Vereinbarungen von Kaspersky der Benutzer akzeptiert hat.

- Die Daten des Administrationsservers, die der Benutzer in der Kaspersky Security Center Web Console oder in der Programmschnittstelle Kaspersky Security Center OpenAPI eingibt.

- Alle Daten, die der Benutzer auf der Benutzeroberfläche von Kaspersky Security Center Web Console eingibt.

Die oben aufgeführten Daten können in Kaspersky Security Center Linux vorhanden sein, wenn eine der folgenden Methoden verwendet wird:

- Der Benutzer gibt Daten in die Oberfläche der Kaspersky Security Center Web Console ein.

- Der Administrationsagent empfängt Daten automatisch vom Gerät und überträgt diese an den Administrationsserver.

- Der Administrationsagent empfängt von der durch Kaspersky verwalteten Anwendung abgerufenen Daten und überträgt sie an den Administrationsserver. Die Liste der verarbeiteten Daten von der durch Kaspersky verwalteten Anwendungen finden Sie in der Hilfe der entsprechenden Anwendungen.

- Der Administrationsserver bezieht die Informationen über die vernetzten Geräte entweder selbst oder erhält sie von einem Administrationsagenten, der als Verteilungspunkt fungiert.

- Daten werden vom mobilen Gerät zum Administrationsserver mittels iOS MDM-Protokoll oder mobilen Protokoll übertragen.

Die aufgelisteten Daten werden in der Administrationsserver-Datenbank gespeichert. Hashes von Kennwörtern werden verschlüsselt gespeichert.

Alle lokal verarbeiteten Daten, einschließlich Protokolldateien, die von Installationsprogrammen und Dienstprogrammen erstellt wurden, können nur mittels Dump-Dateien, Protokolldateien oder Log-Dateien von Komponenten von Kaspersky Security Center Linux übertragen werden.

Die Dump-, Trace- oder Protokolldateien der Linux-Komponenten von Kaspersky Security Center enthalten willkürliche Daten des Administrationsservers, des Administrationsagenten und der Kaspersky Security Center Web Console. Die Dateien können persönliche oder vertrauliche Daten enthalten. Die Dump-, Protokoll- und Log-Dateien werden unverschlüsselt auf dem Gerät gespeichert. Die Dump-, Protokoll- und Log-Dateien werden nicht automatisch an Kaspersky übertragen. Der Administrator kann jedoch auf Anforderung des Technischen Supports Daten manuell an Kaspersky übertragen, um Probleme bei Ausführung von Kaspersky Security Center Linux zu beheben.

Kaspersky schützt alle erhaltenen Informationen in Übereinstimmung mit den geltenden Gesetzen und geltenden Kaspersky-Regeln. Daten werden über einen sicheren Kanal übertragen.

Durch dem Folgen der Links in der Kaspersky Security Center Web Console stimmt der Nutzer zu, die folgenden Daten automatisch zu übertragen:

- Code von Kaspersky Security Center Linux
- Version von Kaspersky Security Center Linux
- Lokalisierung von Kaspersky Security Center Linux
- Lizenz-ID
- Lizenztyp
- Ob die Lizenz über einen Partner bezogen wurde

Die Liste an Daten, die über einen Link zur Verfügung gestellt werden, ist abhängig von Zweck und Standort des Links.

Kaspersky verwendet die erhaltenen Daten in anonymisierter Form und nur für allgemeine Statistiken. Zusammenfassende Statistiken werden automatisch aus den ursprünglich erhaltenen Informationen erstellt und enthalten keine persönlichen oder vertraulichen Daten. Sobald neue Daten akkumuliert wurden, werden die vorherigen Daten gelöscht (einmal pro Jahr). Zusammenfassende Statistiken werden unbegrenzt gespeichert.

Über das Abonnement

Ein *Abonnement für Kaspersky Security Center Linux* ist eine Bestellung der Anwendung mit bestimmten Einstellungen (Ablaufdatum des Abonnements, Anzahl der geschützten Geräte). Ein Abonnement für Kaspersky Security Center Linux kann bei einem Lieferanten von Dienstleistungen abgeschlossen werden (z. B. bei einem Internet-Provider). Das Abonnement kann manuell oder automatisch verlängert oder auch gekündigt werden.

Ein Abonnement kann beschränkt (z. B. auf ein Jahr) oder unbeschränkt (ohne Ablaufdatum) sein. Um Kaspersky Security Center weiterhin zu nutzen, muss ein beschränktes Abonnement rechtzeitig verlängert werden. Ein unbeschränktes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag rechtzeitig an den Dienstleister überwiesen wird.

Nach Ablauf eines befristeten Abonnements wird möglicherweise eine Nachfrist zur Abonnement-Verlängerung gewährt, innerhalb dieser die Funktionalität der Anwendung erhalten bleibt. Verfügbarkeit und Dauer der Nachfrist werden vom Lieferanten der Dienstleistungen bestimmt.

Um Kaspersky Security Center Linux mit einem Abonnement zu nutzen, muss der Aktivierungscode übernommen werden, den Sie von Ihrem Provider erhalten.

Sie können nur dann einen anderen Aktivierungscode für die Nutzung von Kaspersky Security Center Linux verwenden, wenn das Abonnement zuvor abgelaufen ist oder gekündigt wurde.

Für die Abonnement-Verwaltung stehen je nach Provider unterschiedliche Optionen zur Verfügung. Der Provider stellt möglicherweise keine Nachfrist für die Verlängerung des Abonnements zur Verfügung, innerhalb der die Funktionen der Anwendung erhalten bleiben.

Die für ein Abonnement erhaltenen Aktivierungscodes können nicht für die Aktivierung vorheriger Versionen von Kaspersky Security Center verwendet werden.

Bei einer Nutzung der Anwendung im Abonnement stellt Kaspersky Security Center Linux zum festgelegten Zeitpunkt vor Ablauf des Abonnements automatisch eine Verbindung zum Aktivierungsserver her. Wenn der Zugriff auf den Server über systemspezifisches DNS nicht möglich ist, verwendet die Anwendung öffentliche DNS-Server. Sie können das Abonnement auf der Website des Providers verlängern.

Kaspersky Security Center Linux aktivieren

Sie können Kaspersky Security Center Linux aktivieren, um dessen zusätzlichen Funktionen zu nutzen. Dies kann auf zwei unterschiedliche Weisen getan werden: Sie können entweder den Schnellstartassistenten des Administrationsservers oder die Eigenschaften des Administrationsservers verwenden.

So aktivieren Sie Kaspersky Security Center Linux:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Lizenzschlüssel** aus.

3. Klicken Sie unter **Aktuelle Lizenz** auf die Schaltfläche **Auswählen**.

4. Wählen Sie im angezeigten Fenster den Lizenzschlüssel aus, den Sie für die Aktivierung von Kaspersky Security Center Linux verwenden möchten. Wenn der Lizenzschlüssel nicht aufgeführt ist, klicken Sie auf die Schaltfläche **Neuen Lizenzschlüssel hinzufügen** und geben Sie anschließend einen neuen Lizenzschlüssel ein.

5. Bei Bedarf können Sie auch einen Reserve-Lizenzschlüssel hinzufügen. Klicken Sie dazu unter **Reserve-Lizenzschlüssel** auf die Schaltfläche **Auswählen** und wählen Sie einen vorhandenen Lizenzschlüssel aus oder fügen Sie einen neuen hinzu. Beachten Sie, dass Sie keinen Reserve-Lizenzschlüssel hinzufügen können, wenn kein aktiver Lizenzschlüssel vorhanden ist.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Lizenzierung verwalteter Kaspersky-Anwendungen

Dieser Abschnitt beschreibt die Funktionen von Kaspersky Security Center, die sich auf die Arbeit mit den Lizenzschlüsseln von verwalteten Kaspersky-Anwendungen beziehen.

Kaspersky Security Center Linux ermöglicht eine zentrale Verteilung von Lizenzschlüsseln für Kaspersky-Anwendungen auf Client-Geräte sowie die Überwachung der Schlüsselverwendung und die Verlängerung von Lizenzen.

Beim Hinzufügen eines Lizenzschlüssels über Kaspersky Security Center werden die Lizenzschlüssel-Einstellungen auf dem Administrationsserver gespeichert. Anhand dieser Informationen erstellt die Anwendung einen Bericht über die Nutzung des Lizenzschlüssels und informiert den Administrator über den Ablauf der Gültigkeitsdauer von Lizenzen und eine Überschreitung der in den Lizenzschlüssel-Einstellungen vorgegebenen Lizenzbeschränkungen. Sie können die Einstellungen für Benachrichtigungen über die Nutzung von Lizenzschlüsseln in den Einstellungen des Administrationsservers konfigurieren.

Lizenzierung der verwalteten Programme

Jedes der auf den verwalteten Geräten installierten Kaspersky-Anwendungen muss mit einer Schlüsseldatei oder einem Aktivierungscode lizenziert werden. Eine Schlüsseldatei oder ein Aktivierungscode kann folgendermaßen bereitgestellt werden:

- Mittels automatischer Verteilung
- Mittels Installationspaket der verwalteten Anwendung
- Mittels der Aufgabe "Lizenzschlüssel hinzufügen" für eine verwaltete Anwendung
- Mittels manueller Aktivierung einer verwalteten Anwendung

Sie können mit einer der oben aufgeführten Methoden einen neuen aktiven Lizenzschlüssel oder einen Reserve-Lizenzschlüssel hinzufügen. Kaspersky-Anwendungen verwenden zum aktuellen Zeitpunkt einen aktiven Schlüssel und speichern einen Reserveschlüssel, der nach Ablauf des aktiven Schlüssels angewendet wird. Die Anwendung, für welche Sie einen Lizenzschlüssel hinzufügen, definiert, ob der Schlüssel aktiv oder reserviert ist. Die Definition des Schlüssels hängt nicht von der Methode ab, die Sie zum Hinzufügen des neuen Lizenzschlüssels verwenden.

Mittels automatischer Verteilung

Wenn Sie verschiedene verwaltete Anwendungen verwenden und eine bestimmte Schlüsseldatei oder Aktivierungscode an die Geräte verteilen möchten, verwenden Sie andere Methoden zur Verteilung des Aktivierungscodes oder der Schlüsseldatei.

Kaspersky Security Center erlaubt die automatische Verteilung der vorhandenen Lizenzschlüssel an die Geräte. Angenommen, in der Datenverwaltung des Administrationsservers befinden sich drei Lizenzschlüssel. Sie haben die Option **Automatisch verteilter Lizenzschlüssel** für alle drei Lizenzschlüssel aktiviert. Auf den Unternehmensgeräten ist eine Sicherheitsanwendung von Kaspersky installiert, z. B. Kaspersky Endpoint Security für Linux. Ein neues Gerät wurde entdeckt und erfordert die Bereitstellung eines Lizenzschlüssels. Die Anwendung ermittelt, dass für dieses Gerät z. B. zwei Lizenzschlüssel aus dem Speicher geeignet sind: Lizenzschlüssel *Key_1* und Lizenzschlüssel *Key_2*. Einer dieser Lizenzschlüssel wird an das Gerät verteilt. In diesem Fall kann nicht vorausgesagt werden, welcher der beiden Lizenzschlüssel an das Gerät bereitgestellt werden wird, da die automatische Verteilung von Lizenzschlüsseln keinerlei Aktivitäten des Administrators vorsieht.

Bei der Verteilung des Lizenzschlüssels an das Gerät erfolgt eine Zählung aller Geräte, für die dieser Schlüssel gilt. Sie müssen sicherstellen, dass die Anzahl der Geräte, an die der Lizenzschlüssel verteilt wird, die Lizenzbeschränkung nicht überschreitet. Falls die Anzahl der Geräte die Lizenzbeschränkung überschreitet, wird allen Geräten, die nicht durch die Lizenz abgedeckt sind, der Status *Kritisch* zugewiesen.

Vor der Verteilung muss die Schlüsseldatei oder Aktivierungscode zur Datenverwaltung des Administrationsservers hinzugefügt werden.

Anleitung:

- Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
- Lizenzschlüssel automatisch verteilen

Beachten Sie, dass ein automatisch verteilter Lizenzschlüssel in den folgenden Fällen möglicherweise nicht in der Datenverwaltung des virtuellen Administrationsservers angezeigt wird:

- Der Lizenzschlüssel ist nicht für diese Anwendung vorgesehen.
- Der virtuelle Administrationsserver verfügt über keine verwalteten Geräte.
- Der Lizenzschlüssel wird bereits für Geräte verwendet, die unter Verwaltung eines anderen virtuellen Administrationsservers stehen, und die maximale Anzahl an Geräten wurde erreicht.

Hinzufügen einer Schlüsseldatei oder eines Aktivierungscodes zum Installationspaket einer verwalteten Anwendung

Diese Option wird aus Sicherheitsgründen nicht empfohlen. Eine Schlüsseldatei oder ein Aktivierungscode, der zum Installationspaket hinzugefügt wurde, kann kompromittiert werden.

Wenn die Installation der verwalteten Anwendung mithilfe eines Installationspakets erfolgt, können Sie eine Schlüsseldatei oder einen Aktivierungscode im Installationspaket oder in der Richtlinie dieser Anwendung angeben. Der Lizenzschlüssel wird bei der nächsten Synchronisierung des Geräts mit dem Administrationsserver an die verwalteten Geräte verteilt.

Anleitungen: Lizenzschlüssel zu einem Installationspaket hinzufügen

Verteilung mithilfe der Aufgabe zum Hinzufügen eines Lizenzschlüssels für eine verwaltete Anwendung

Wenn Sie die Aufgabe zum Hinzufügen eines Lizenzschlüssels für verwaltete Anwendungen verwenden, können Sie den Lizenzschlüssel auswählen, der an die Geräte verteilt werden soll, und die Geräte auf die von Ihnen bevorzugte Art auswählen, z. B. indem Sie eine Administrationsgruppe oder eine Geräteauswahl wählen.

Vor der Verteilung muss die Schlüsseldatei oder Aktivierungscode zur Datenverwaltung des Administrationsservers hinzugefügt werden.

Anleitung:

- Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen
- Lizenzschlüssel auf Client-Geräte verteilen

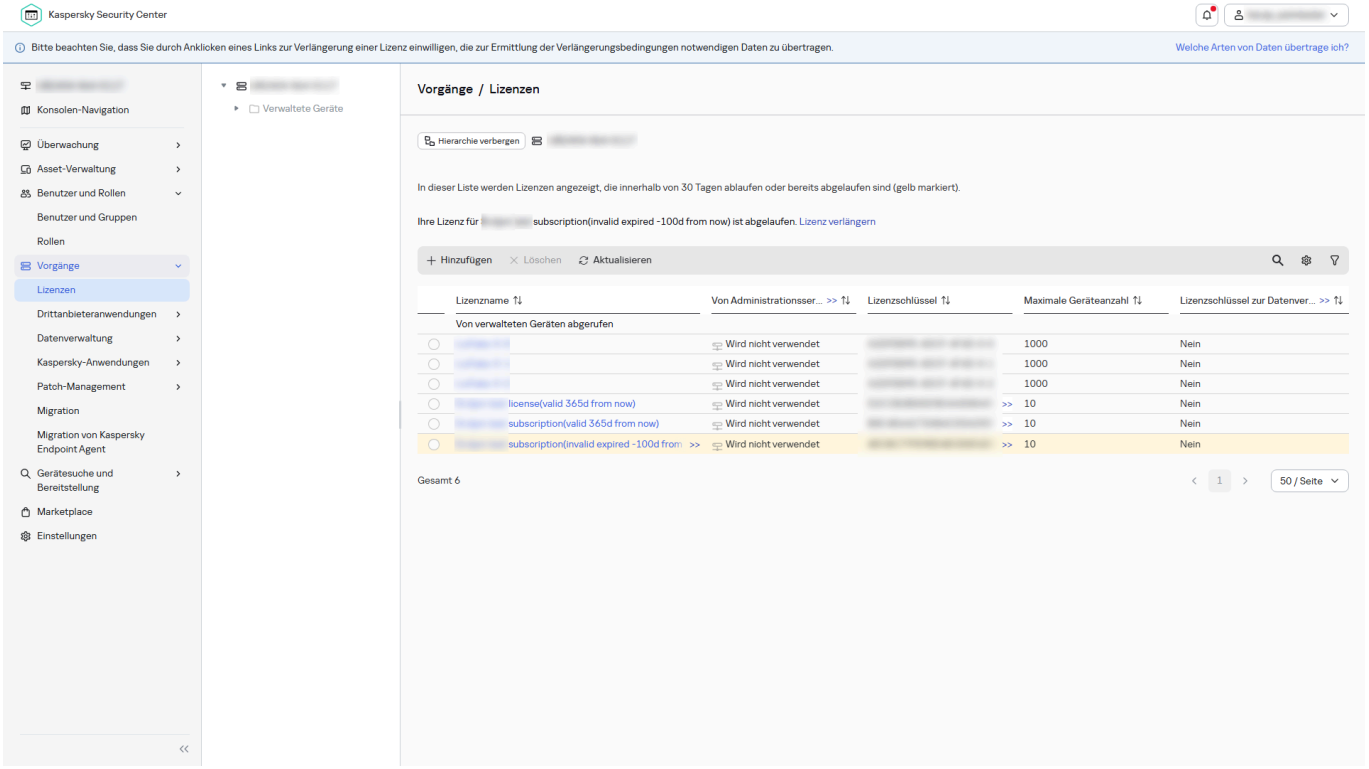
Manuelles Hinzufügen des Aktivierungscodes oder der Schlüsseldatei auf den Geräten.

Sie können die installierte Kaspersky-Anwendung lokal mittels der Tools in der Programmoberfläche aktivieren. Weitere Informationen finden Sie in der Dokumentation zur installierten Anwendung.

Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen

Um einen Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzuzufügen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Lizenzen**.



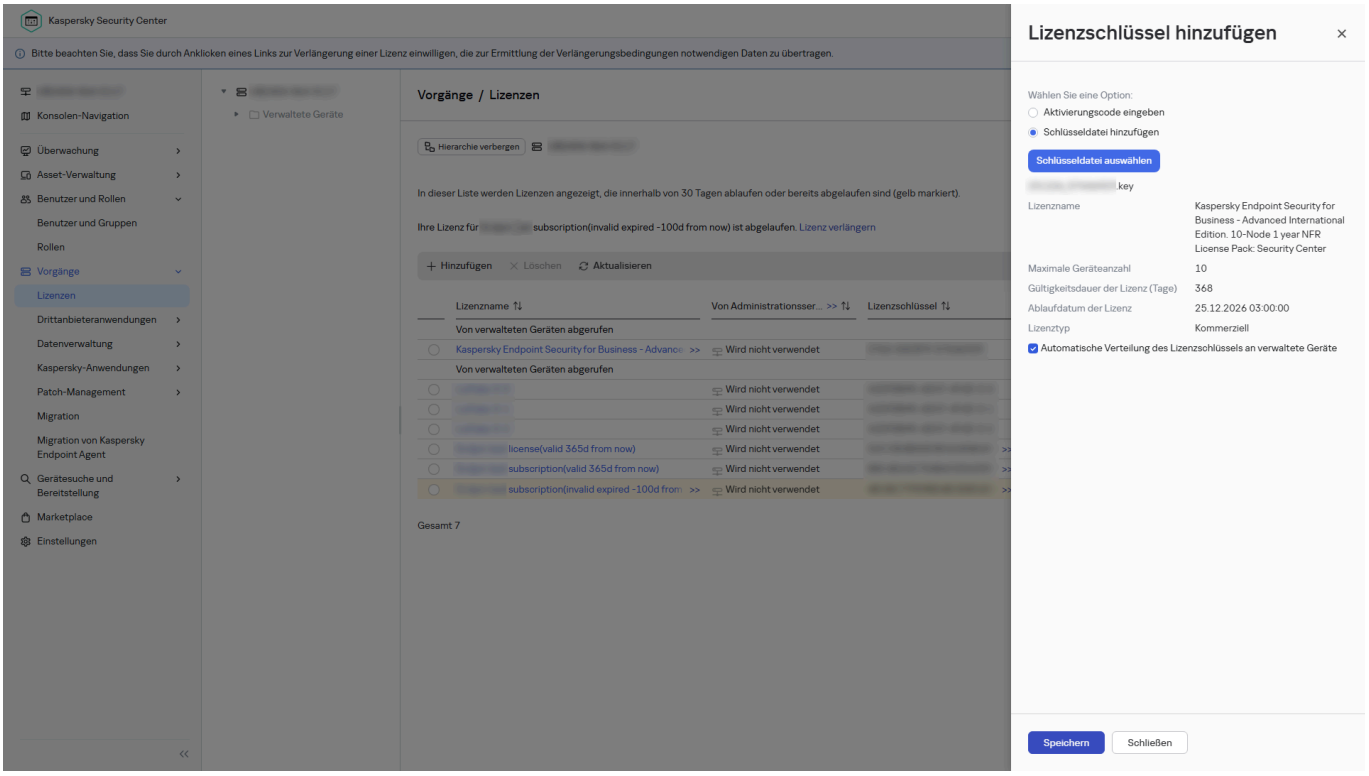
Liste der hinzugefügten Kaspersky-Lizenzschlüssel

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Wählen Sie, was Sie hinzufügen möchten:

- **Schlüsseldatei hinzufügen**

  Klicken Sie auf **Schlüsseldatei auswählen** und finden Sie die .key-Datei, die Sie hinzufügen möchten.



Hinzufügen eines Lizenzschlüssels mittels einer Schlüsseldatei

- **Aktivierungscode eingeben**

  Geben Sie im Textfeld den Aktivierungscode an und klicken Sie auf **Senden**.

4. Klicken Sie auf die Schaltfläche **Schließen**.

Der oder die Lizenzschlüssel werden zur Datenverwaltung des Administrationsservers hinzugefügt.

Lizenzschlüssel auf Client-Geräte verteilen

Die Kaspersky Security Center Web Console ermöglicht die Verteilung von Lizenzschlüsseln auf Client-Geräte entweder mittels automatischer Verteilung oder mittels der Aufgabe **Anwendungsaktivierung**. Sie können die Aufgabe verwenden, um Schlüssel an eine bestimmte Gerätegruppe zu verteilen. Wenn ein Lizenzschlüssel anhand dieser Aufgabe verteilt wird, werden die Lizenzbeschränkungen für die Anzahl der Geräte nicht berücksichtigt. Verwenden Sie die automatische Verteilung von Schlüsseln, um die Verteilung eines Lizenzschlüssels automatisch einzustellen, wenn die Lizenzbeschränkung erreicht ist.

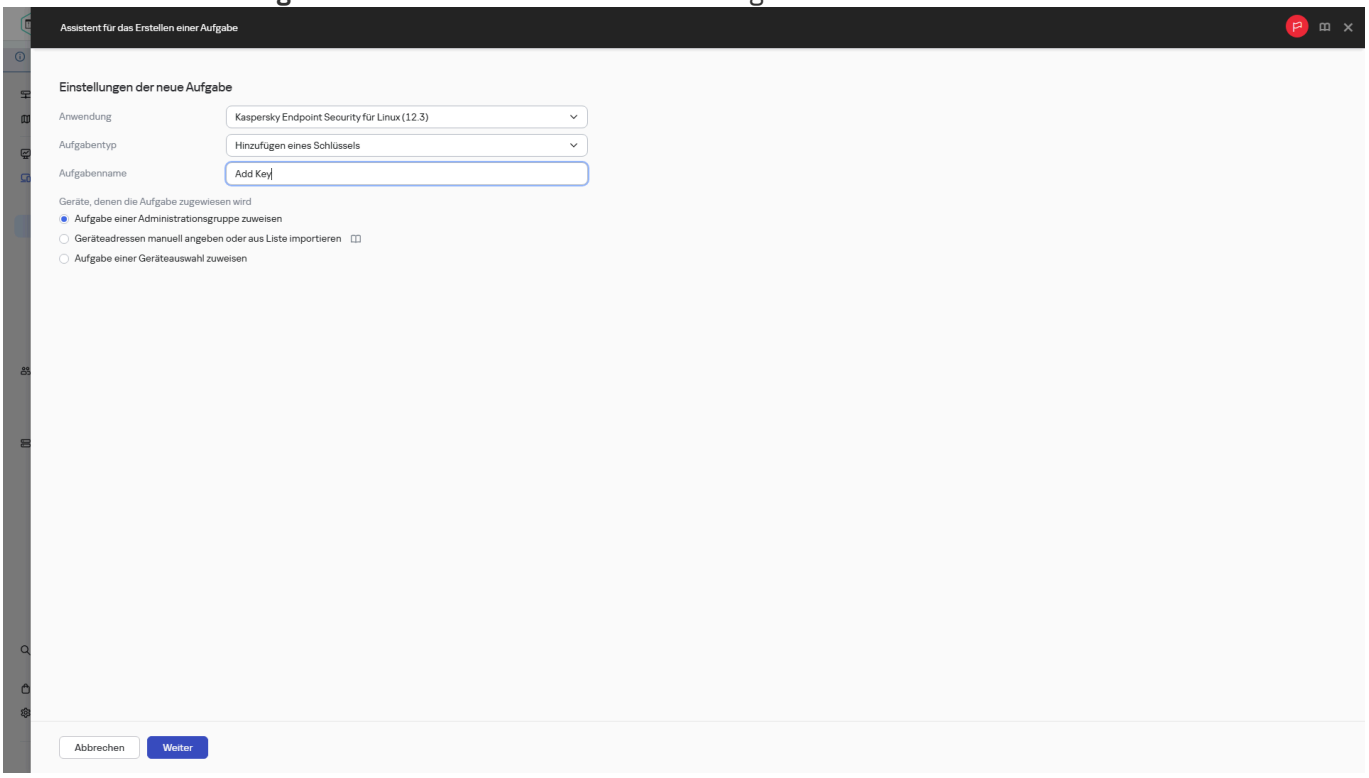
Wenn Sie die automatische Verteilung eines Lizenzschlüssels aktivieren, erstellen Sie keine Aufgabe des Typs **Anwendungsaktivierung**, um diesen Schlüssel an Client-Geräte zu verteilen. Andernfalls erhöht sich die Belastung des Administrationsservers aufgrund häufiger Synchronisierungen.

Vor der Verteilung müssen Sie den Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen.

*So verteilen Sie einen Lizenzschlüssel an Client-Geräte mittels der Aufgabe **Anwendungsaktivierung**:*

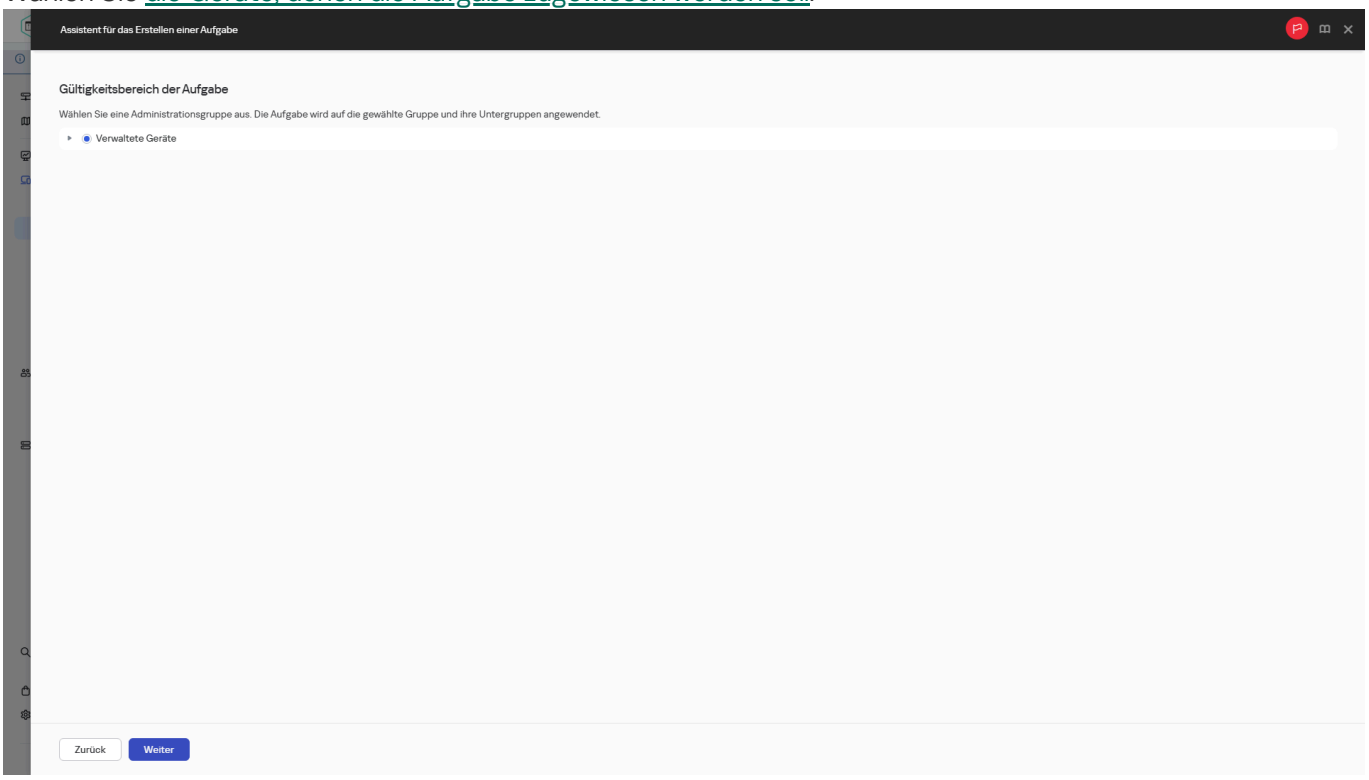
1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der **Assistent für das Erstellen einer Aufgabe** wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
3. Wählen Sie in der Dropdown-Liste **Anwendung** die Anwendung aus, für das Sie einen Lizenzschlüssel hinzufügen möchten.
4. Wählen Sie in der Liste **Aufgabentyp** die Aufgabe **Anwendungsaktivierung** aus.
5. Geben Sie im Feld **Aufgabenname** den Namen der neuen Aufgabe an.



Erstellen einer Aufgabe "Schlüssel hinzufügen"

6. Wählen Sie die Geräte, denen die Aufgabe zugewiesen werden soll.



Angeben des Gültigkeitsbereichs der Aufgabe

7. Klicken Sie im Schritt **Lizenzschlüssel auswählen** des Assistenten auf den Link **Schlüssel hinzufügen**, um den Lizenzschlüssel hinzuzufügen.

8. Fügen Sie im Bereich zum Hinzufügen von Schlüsseln den Lizenzschlüssel mit einer der folgenden Optionen hinzu:

> Sie müssen den Lizenzschlüssel nur dann hinzufügen, wenn Sie ihn vor der Erstellung der Aufgabe **Anwendungsaktivierung** nicht zur Datenverwaltung des Administrationsservers hinzugefügt haben.

- Wählen Sie die Option **Aktivierungscode eingeben**, um einen Aktivierungscode einzugeben, und gehen Sie anschließend wie folgt vor:

  a. Geben Sie den Aktivierungscode ein und klicken Sie anschließend auf die Schaltfläche **Senden**.

  Die Informationen des Lizenzschlüssels werden im Fenster zum Hinzufügen des Schlüssels angezeigt.

  b. Klicken Sie auf die Schaltfläche **Speichern**.

  > Wenn Sie den Lizenzschlüssel automatisch an verwaltete Geräte verteilen möchten, aktivieren Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.

  Der Bereich zum Hinzufügen von Schlüsseln wird geschlossen.

- Wählen Sie die Option **Schlüsseldatei hinzufügen** aus, um eine Schlüsseldatei hinzuzufügen, und gehen Sie anschließend wie folgt vor:

  a. Klicken Sie auf die Schaltfläche **Schlüsseldatei auswählen**.

  b. Wählen Sie in dem sich öffnenden Fenster eine Schlüsseldatei und klicken Sie anschließend auf die Schaltfläche **Öffnen**.

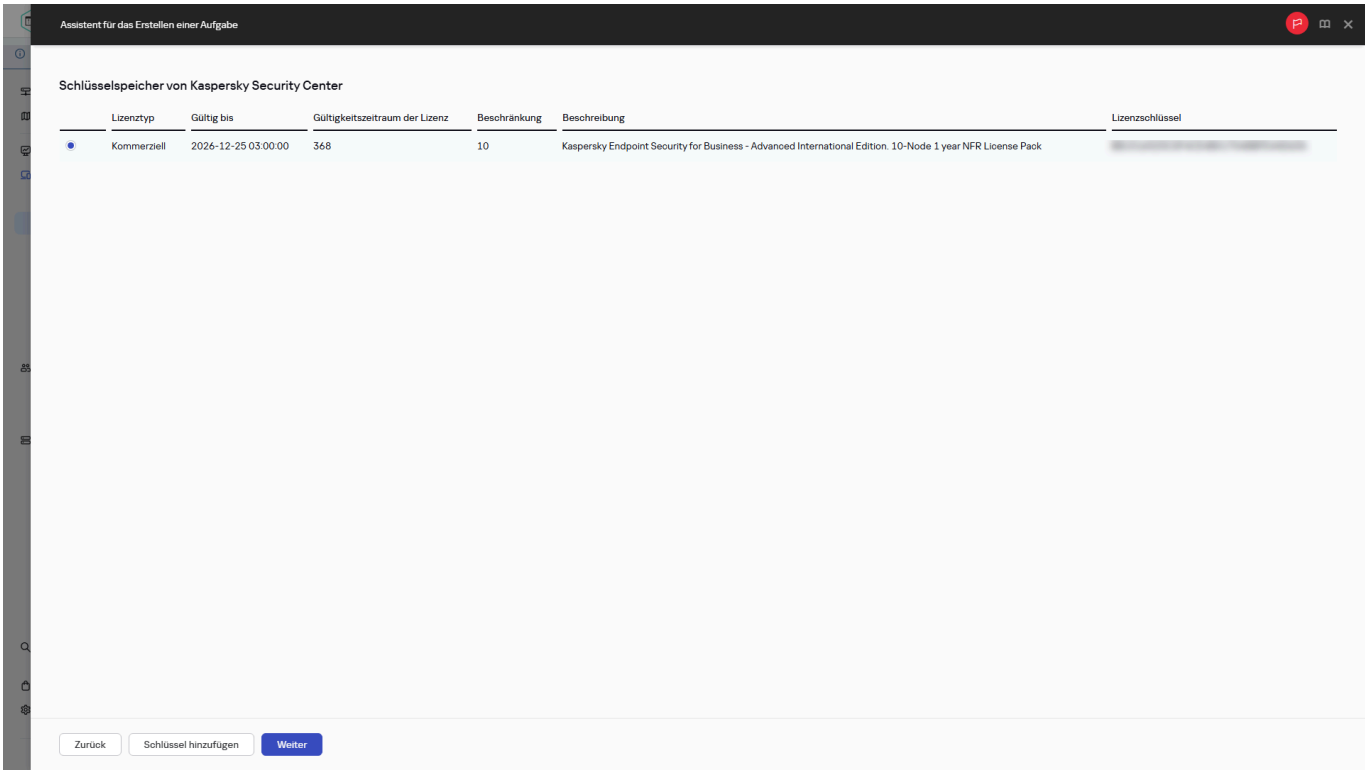
  Die Informationen des Lizenzschlüssels werden im Fenster zum Hinzufügen des Lizenzschlüssels angezeigt.

  c. Klicken Sie auf die Schaltfläche **Speichern**.

  > Wenn Sie den Lizenzschlüssel automatisch an verwaltete Geräte verteilen möchten, aktivieren Sie die Option **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.

  Der Bereich zum Hinzufügen von Schlüsseln wird geschlossen.

9. Wählen Sie in der Tabelle mit Schlüsseln den Lizenzschlüssel aus.

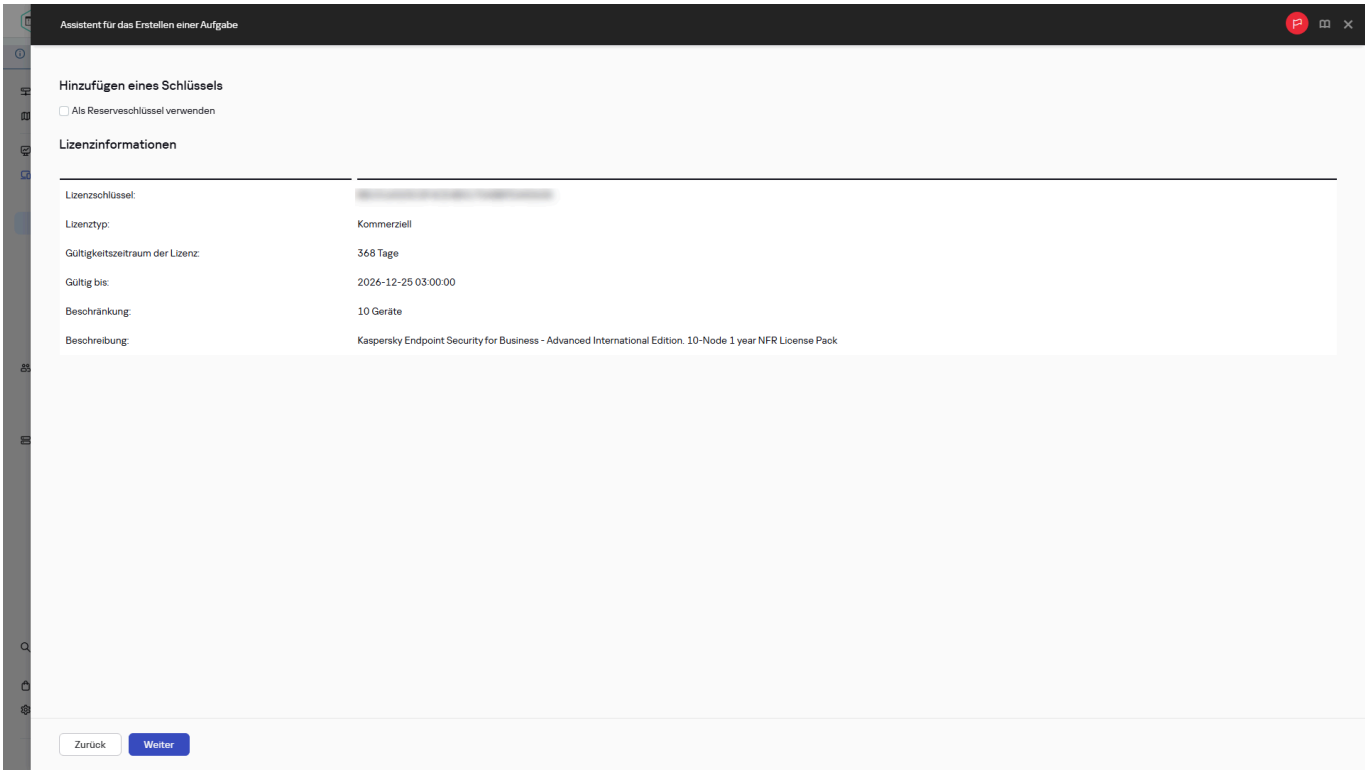


Auswahl des Lizenzschlüssels

10. Wenn Sie den aktiven Lizenzschlüssel ersetzen möchten, deaktivieren Sie im Schritt **Lizenzinformationen** des Assistenten das standardmäßige Kontrollkästchen **Als Reserveschlüssel verwenden**.

    Dies kann beispielsweise erforderlich sein, wenn sich die Organisation ändert und der Schlüssel einer anderen Organisation auf dem Gerät benötigt wird; oder wenn der Schlüssel erneut ausgestellt wurde und eine neue Lizenz früher abläuft als die aktuelle Lizenz. Um Fehler zu vermeiden, müssen Sie das Kontrollkästchen **Als Reserveschlüssel verwenden** deaktivieren.

Weitere Informationen über Probleme, die beim Hinzufügen eines Lizenzschlüssels zu Kaspersky Security Center auftreten können, sowie Möglichkeiten, diese Probleme zu beheben, finden Sie in der Wissensdatenbank von Kaspersky Security Center.



Angeben des Reserve-Lizenzschlüssels

11. Aktivieren Sie beim Schritt **Erstellung der Aufgabe abschließen** des Assistenten die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**, um die standardmäßigen Aufgabeneinstellungen zu ändern.

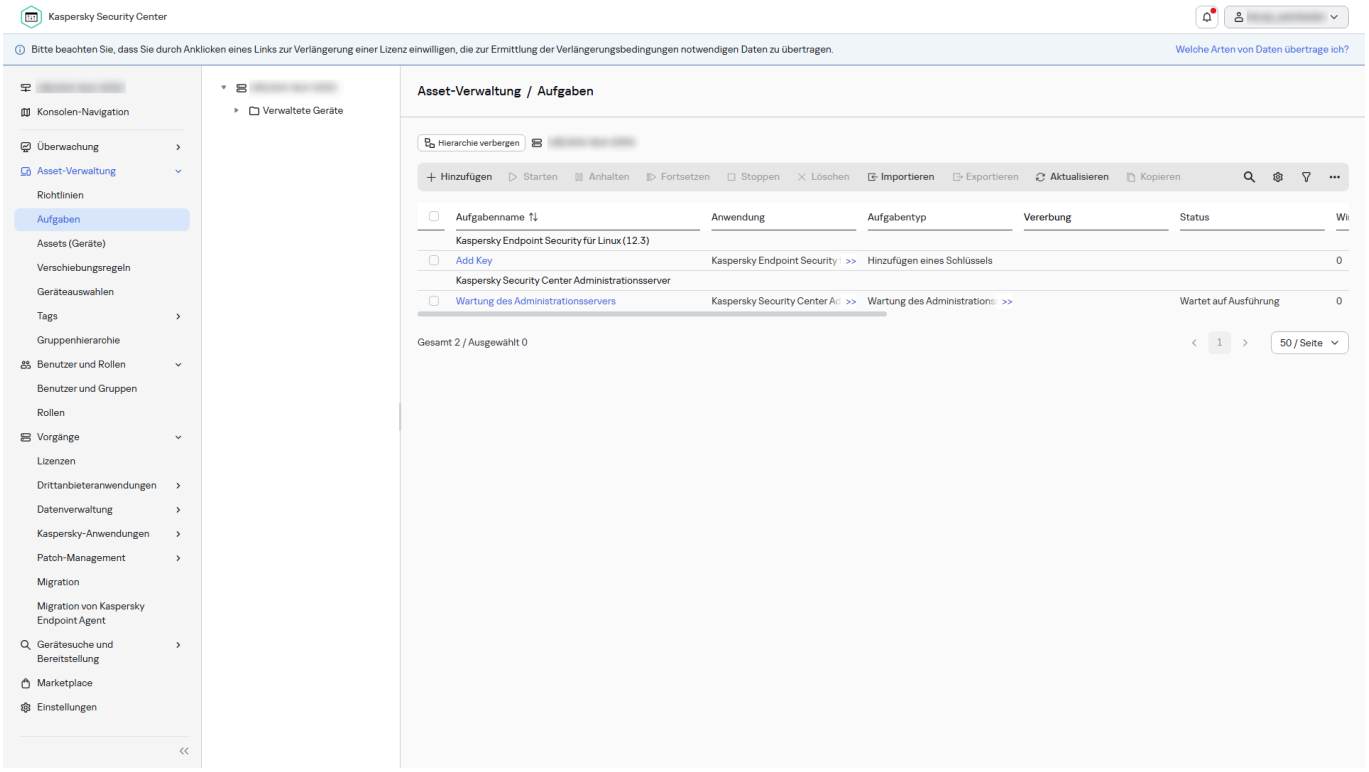
    Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später ändern.

12. Klicken Sie auf die Schaltfläche **Fertigstellen**.

    Der Assistent erstellt die Aufgabe. Wenn Sie die Option Nach **Nach Abschluss der Erstellung Aufgabendetails öffnen** haben, wird das Fenster mit Aufgabeneigenschaften automatisch geöffnet. In diesem Fenster können Sie die allgemeinen Aufgabeneinstellungen angeben und bei Bedarf die Einstellungen ändern, die bei der Aufgabenerstellung festgelegt wurden.

    Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Aufgabenliste auf den Namen der erstellten Aufgabe klicken.

Die Aufgabe wurde erstellt und konfiguriert und wird in der Aufgabenliste angezeigt.



Die Aufgabenliste

13. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf **Starten**.

    Auf der Registerkarte **Zeitplan** im Eigenschaftenfenster der Aufgabe können Sie auch einen Zeitplan für den Aufgabenstart festlegen.

    Eine detaillierte Beschreibung der Einstellungen für das Starten nach Zeitplan finden Sie in den allgemeinen Aufgabeneinstellungen.

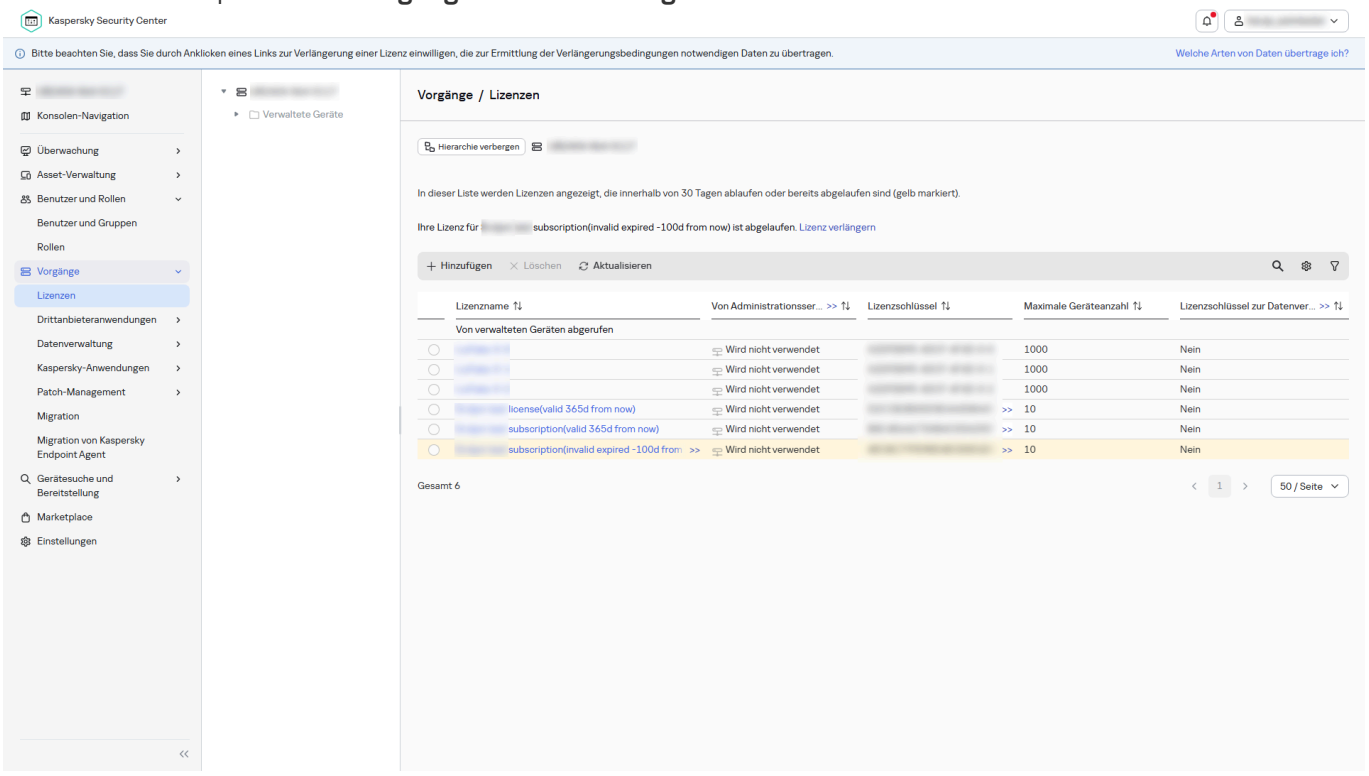
Nachdem dem Abschluss der Aufgabe ist der Lizenzschlüssel auf den ausgewählten Geräten bereitgestellt.

Lizenzschlüssel automatisch verteilen

Kaspersky Security Center Linux ermöglicht das automatische Verteilen von Lizenzschlüsseln, die sich im Schlüsselspeicher auf dem Administrationsserver befinden, auf die verwalteten Geräte.

Um einen Lizenzschlüssel automatisch auf die verwalteten Geräte zu verteilen, gehen Sie wie folgt vor:

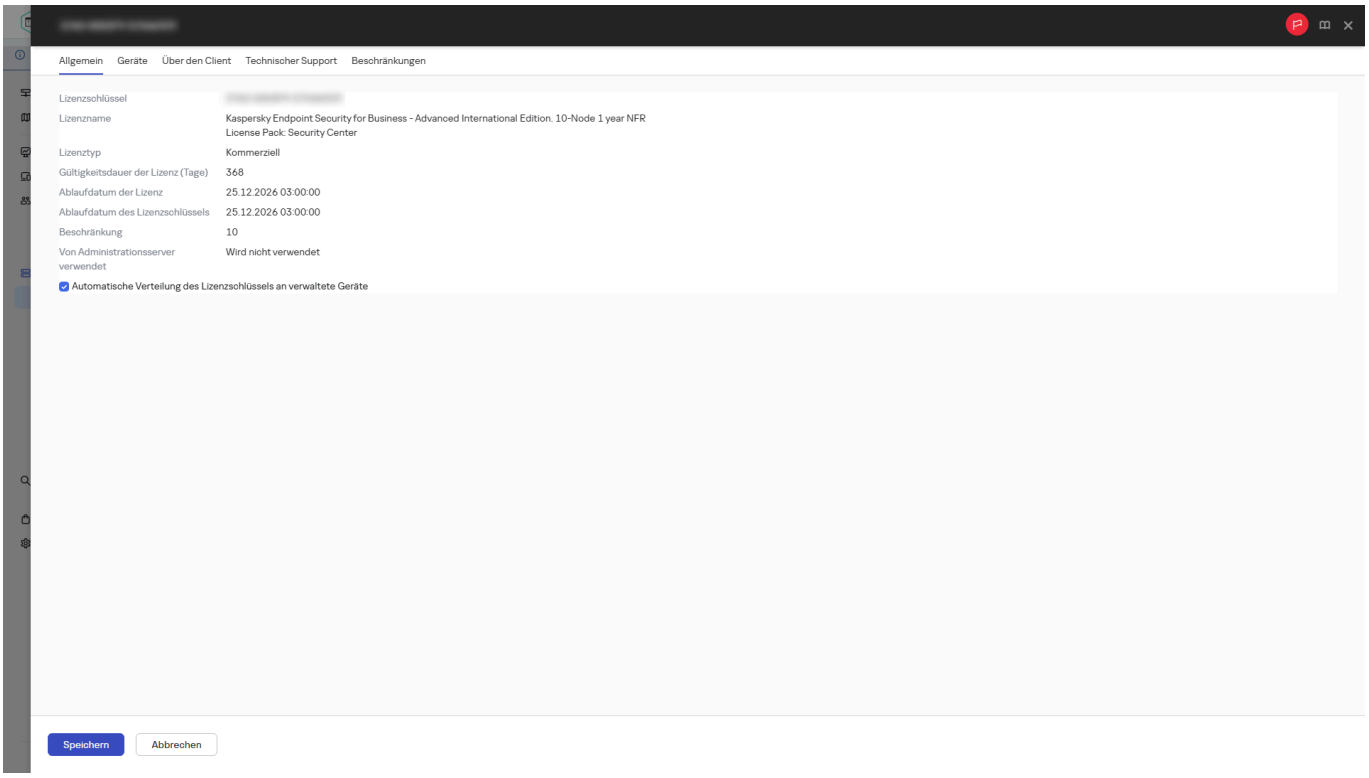
1. Gehen Sie im Hauptmenü zu **Vorgänge → Lizenzierung → Lizenzen**.



Die Liste der Lizenzen

2. Klicken Sie auf den Namen des Lizenzschlüssels, den Sie automatisch auf die Geräte verteilen möchten.

3. Aktivieren Sie im folgenden Eigenschaftenfenster des Lizenzschlüssels **Lizenzschlüssel automatisch an verwaltete Geräte verteilen**.



Das Eigenschaftsfenster des Lizenzschlüssels

4. Klicken Sie auf die Schaltfläche **Speichern**.

Der Lizenzschlüssel wird automatisch an alle kompatiblen Geräte verteilt.

Die Verteilung des Lizenzschlüssels erfolgt durch den Administrationsagenten. Für die Anwendung werden keine Aufgaben zur Verteilung eines Lizenzschlüssels erstellt.

Wenn ein Lizenzschlüssel automatisch verteilt wird, werden die Lizenzbeschränkungen für die Anzahl der Geräte berücksichtigt. Die Beschränkung ist in den Eigenschaften des Lizenzschlüssels festgelegt. Wenn die Lizenzbeschränkung erreicht ist, wird die Verteilung des Lizenzschlüssels auf Geräte automatisch beendet.

Beachten Sie, dass ein automatisch verteilter Lizenzschlüssel in den folgenden Fällen möglicherweise nicht in der Datenverwaltung des virtuellen Administrationsservers angezeigt wird:

- Der Lizenzschlüssel ist nicht für diese Anwendung vorgesehen.
- Der virtuelle Administrationsserver verfügt über keine verwalteten Geräte.
- Der Lizenzschlüssel wird bereits für Geräte verwendet, die unter Verwaltung eines anderen virtuellen Administrationsservers stehen, und die maximale Anzahl an Geräten wurde erreicht.

Der virtuelle Administrationsserver verteilt Lizenzschlüssel aus seiner Datenverwaltung und aus der Datenverwaltung des Administrationsservers automatisch. Es wird folgendes Vorgehen empfohlen:

- Verwenden Sie die Aufgabe *Lizenzschlüssel hinzufügen*, um den Lizenzschlüssel auszuwählen, der auf den Geräten verteilt werden soll.
- Vermeiden Sie das Deaktivieren der Option **Automatische Verteilung der Lizenzschlüssel auf die Geräte dieses virtuellen Administrationsservers zulassen** in den Einstellungen des virtuellen Administrationsservers. Andernfalls verteilt der virtuelle Administrationsserver keine Lizenzschlüssel an die Geräte (auch nicht jene Lizenzschlüssel, die sich in der Datenverwaltung des Administrationsservers befinden).

Wenn Sie in dem Eigenschaftenfenster des Lizenzschlüssels das Kontrollkästchen **Lizenzschlüssel automatisch an verwaltete Geräte verteilen** auswählen, wird sofort ein Lizenzschlüssel in Ihrem Netzwerk verteilt. Wenn Sie diese Option nicht auswählen, können Sie später eine Aufgabe zur Verteilung der Lizenzschlüssel verwenden.

Die auf dem primären Administrationsserver konfigurierte automatische Verteilung von Lizenzschlüsseln berücksichtigt keine Geräte, die durch nicht-virtuelle sekundäre Administrationsservern verwaltet werden.

Informationen zu verwendeten Lizenzschlüsseln anzeigen

Um die Liste mit Lizenzschlüsseln anzuzeigen, die zur Datenverwaltung des Administrationsservers hinzugefügt wurden, gehen Sie wie folgt vor:

Gehen Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen**.

Die angezeigte Liste enthält die Schlüsseldatei und Aktivierungscodes, die zur Datenverwaltung des Administrationsservers hinzugefügt wurden.

Um detaillierte Informationen über einen Lizenzschlüssel anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen**.
2. Klicken Sie auf den Namen des gewünschten Lizenzschlüssels.

Im Eigenschaftenfenster des Lizenzschlüssels können Sie Folgendes ansehen:

- Auf der Registerkarte **Allgemein**: die wichtigsten Informationen über den Lizenzschlüssel
- Auf der Registerkarte **Geräte**: die Liste mit Client-Geräten, auf denen der Lizenzschlüssel für die Aktivierung der installierten Kaspersky-Anwendung verwendet wurde
- Auf der Registerkarte **Beschränkungen**: die Liste der Lizenzbeschränkungen

  Wenn Sie den Administrationsserver unter einer Lizenz von Kaspersky Next XDR Optimum aktiviert haben, wird auf der Registerkarte **Beschränkungen** das Feld **XDR-O** mit dem Wert **Enabled** angezeigt.

Um zu sehen, welche Lizenzschlüssel auf einem bestimmten Client-Gerät bereitgestellt werden, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.
2. Klicken Sie auf den Namen des gewünschten Geräts.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Anwendungen** aus.

4. Klicken Sie auf den Namen der Anwendung, für das Sie Informationen über den Lizenzschlüssel anzeigen möchten.

5. Wählen Sie im folgenden Fenster mit den Anwendungseigenschaften die Registerkarte **Allgemein** und öffnen Sie dann den Abschnitt **Lizenz**.

Die wichtigsten Informationen über den aktiven Lizenzschlüssel und die Reserveschlüssel werden angezeigt.

Zur Bestimmung der aktuellen Einstellungen für die Lizenzschlüssel des virtuellen Administrationsservers sendet der Administrationsserver mindestens einmal pro Stunde eine Anfrage an die Aktivierungsserver von Kaspersky. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet die Anwendung öffentliche DNS-Server.

Ereignisse bei Überschreitung der Lizenzbeschränkung

Kaspersky Security Center Linux ermöglicht den automatischen Empfang von Informationen über Ereignisse der Überschreitung der Lizenzbeschränkung von Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind.

Die Ereigniskategorie für die Überschreitung der Lizenzbeschränkung wird anhand folgender Regeln bestimmt:

- Wenn die Anzahl der verwendeten Lizenzeinheiten einer Lizenz zwischen 90% und 100% der Gesamtmenge der Lizenzeinheiten dieser Lizenz liegt, wird das Ereignis in der Ereigniskategorie **Infomeldung** veröffentlicht.

- Wenn die Anzahl der verwendeten Lizenzeinheiten einer Lizenz zwischen 100% und 110% der Gesamtmenge der Lizenzeinheiten dieser Lizenz liegt, wird das Ereignis in der Ereigniskategorie **Warnung** veröffentlicht.

- Wenn die Anzahl der verwendeten Lizenzeinheiten einer Lizenz 110% der Gesamtmenge der Lizenzeinheiten dieser Lizenz übersteigt, wird das Ereignis in der Ereigniskategorie **Kritisches Ereignis** veröffentlicht.

Lizenzschlüssel aus der Datenverwaltung löschen

Wenn Sie den aktiven Lizenzschlüssel löschen, der auf einem verwalteten Gerät bereitgestellt wird, bleibt die Anwendung auf dem verwalteten Gerät weiterhin funktionsfähig.

Um eine Schlüsseldatei oder einen Aktivierungscode aus der Datenverwaltung des Administrationsservers zu löschen, gehen Sie wie folgt vor:

1. Prüfen Sie, dass die Schlüsseldatei oder der Aktivierungscode, den Sie löschen wollen, nicht vom Administrationsserver verwendet wird. Wenn der Administrationsserver den Schlüssel verwendet, können Sie ihn nicht löschen. So können Sie dies prüfen:

   a. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

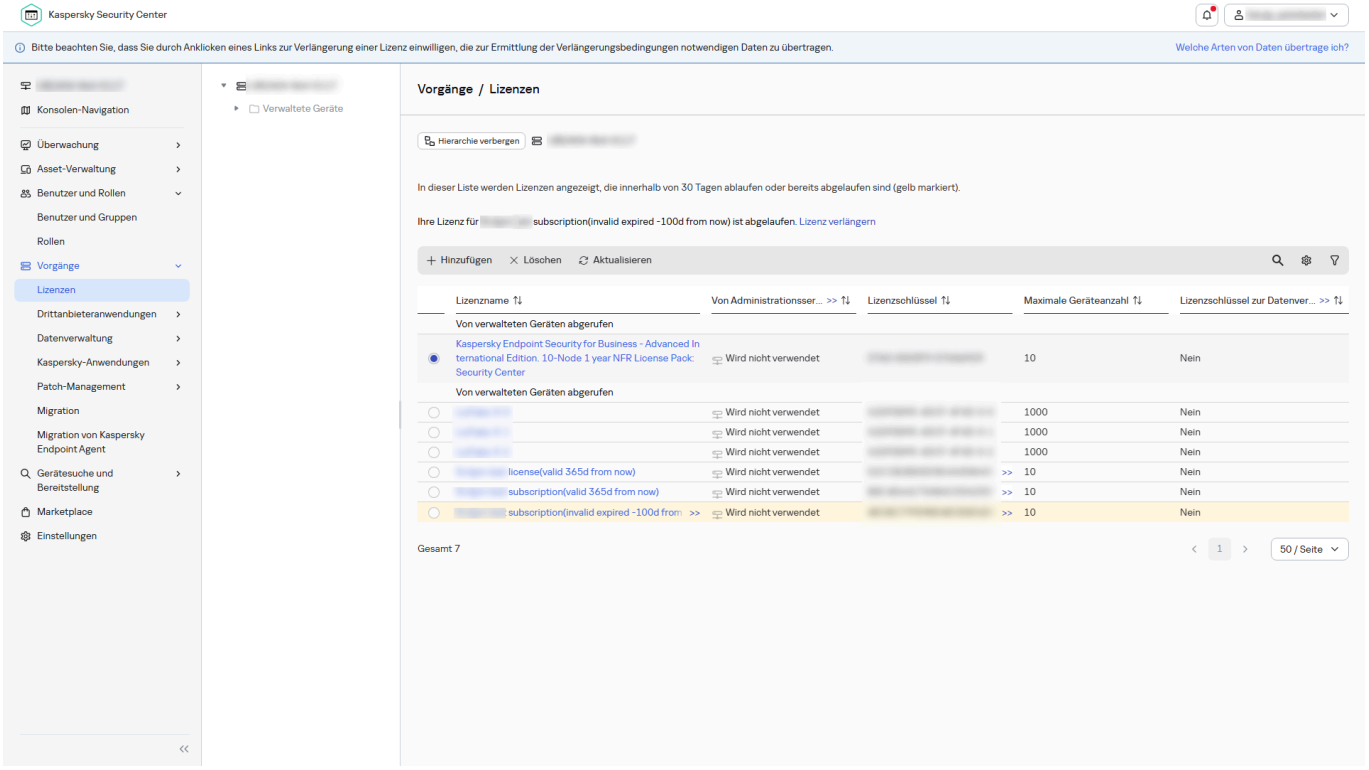
      Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

b. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Lizenzschlüssel** aus.

c. Wenn die erforderliche Schlüsseldatei oder der Aktivierungscode in dem geöffneten Abschnitt angezeigt wird, klicken Sie auf die Schaltfläche **Aktiven Lizenzschlüssel entfernen** und bestätigen Sie den Vorgang. Anschließend wird der gelöschte Lizenzschlüssel nicht mehr vom Administrationsserver verwendet, befindet sich aber weiterhin in der Datenverwaltung des Administrationsservers. Wird die erforderliche Schlüsseldatei oder der Aktivierungscode nicht angezeigt, so wird er vom Administrationsserver nicht verwendet.

2. Gehen Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen**.

3. Wählen Sie die erforderliche Schlüsseldatei oder den Aktivierungscode aus und klicken Sie anschließend auf die Schaltfläche **Löschen**.



Die Liste der Lizenzen

Die ausgewählte Schlüsseldatei oder der Aktivierungscode wird aus der Datenverwaltung gelöscht.

Ein gelöschter Lizenzschlüssel kann erneut hinzugefügt werden, oder es kann ein anderer Lizenzschlüssel hinzugefügt werden.

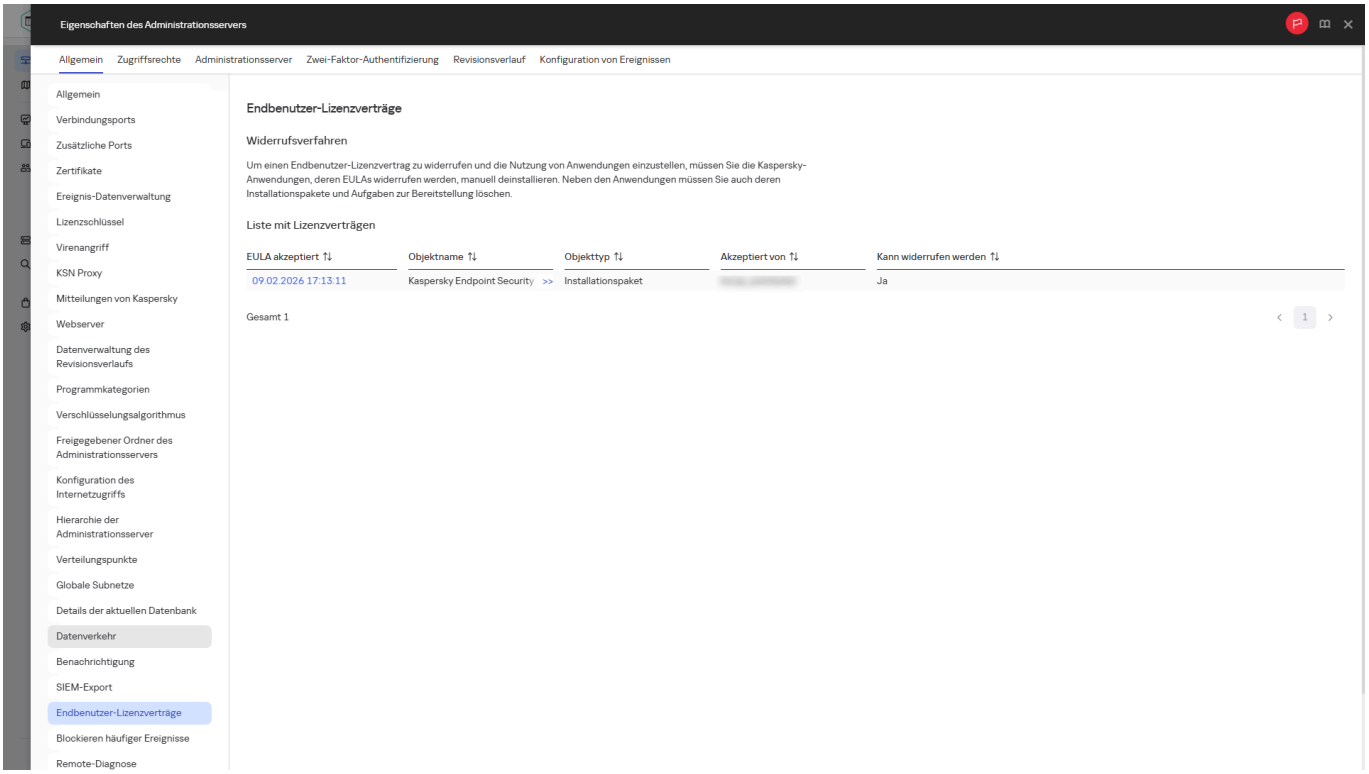
Vereinbarung mit einem Endbenutzer-Lizenzvertrag widerrufen

Wenn Sie sich entschließen, den Schutz für einige Ihrer Client-Geräte zu beenden, können Sie den Endbenutzer-Lizenzvertrag (EULA) für jede verwaltete Kaspersky-Anwendung widerrufen. Vor dem Widerruf der EULA müssen Sie die ausgewählte Anwendung deinstallieren.

So widerrufen Sie eine EULA für verwaltete Kaspersky-Anwendungen:

1. Öffnen Sie das Eigenschaftenfenster des Administrationsservers und wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Endbenutzer-Lizenzverträge**.

Es wird eine Liste der EULAs angezeigt, die beim Erstellen von Installationspaketen, bei der nahtlosen Installation von Updates oder bei der Bereitstellung von Kaspersky Security für mobile Endgeräte akzeptiert wurden.



Die EULA-Liste

2. Wählen Sie in der Liste die EULA aus, die Sie widerrufen möchten.

   Sie können die folgenden Eigenschaften der EULA anzeigen:

   - Datum, an dem die EULA akzeptiert wurde.
   - Name des Benutzers, der die EULA akzeptiert hat.

3. Klicken Sie auf das Datum, an dem die EULA akzeptiert wurde, um ihr Eigenschaftenfenster mit den folgenden Informationen anzuzeigen:

   - Name des Benutzers, der die EULA akzeptiert hat.
   - Datum, an dem die EULA akzeptiert wurde.
   - Eindeutige ID (UID) der EULA.
   - Vollständiger Text der EULA.
   - Liste der mit der EULA verbundenen Objekte (Installationspakete, nahtlose Updates, Mobile Apps) und ihrer entsprechenden Namen und Typen.

4. Klicken Sie im unteren Teil des EULA-Eigenschaftenfensters auf die Schaltfläche **Lizenzvertrag widerrufen**.

   Sollten Objekte (Installationspakete und ihre entsprechenden Aufgaben) existieren, die den Widerruf der EULA verhindern, wird eine entsprechende Nachricht angezeigt. Sie können den Widerruf erst fortsetzen, wenn Sie diese Objekte gelöscht haben.

In dem sich öffnenden Fenster werden Sie darüber informiert, dass Sie zunächst die Kaspersky-Anwendung deinstallieren müssen, welches dieser EULA entspricht.

5. Klicken Sie auf die Schaltfläche, um den Widerruf zu bestätigen.

Die EULA wurde widerrufen. Sie wird nicht länger in der Liste der Endbenutzer-Lizenzverträge im Abschnitt **Endbenutzer-Lizenzverträge** angezeigt. Das EULA-Eigenschaftenfenster schließt sich und die Anwendung ist deinstalliert.

Lizenzen für Kaspersky-Anwendungen verlängern

Lizenzen für Kaspersky-Anwendungen, die entweder abgelaufen oder kurz vor dem Ablaufen sind (weniger als 30 Tage verbleibend) können verlängert werden.

So verlängern Sie Lizenzen, die entweder abgelaufen oder kurz vor dem Ablaufen sind:

1. Führen Sie eine beliebige der folgenden Aktionen aus:

   - Gehen Sie im Hauptmenü zu **Vorgänge → Lizenzierung → Lizenzen**.
   - Wechseln Sie im Hauptmenü zu **Überwachung → Dashboard** und klicken Sie anschließend auf den Link **Ablaufende Lizenzen anzeigen** neben einer Benachrichtigung.

   Es öffnet sich das Fenster **Lizenzen**, in dem Sie Lizenzen anzeigen und erneuern können.

2. Klicken Sie neben der erforderlichen Lizenz auf den Link **Lizenz verlängern**.

   Durch Klicken des Links zur Verlängerung der Lizenz erklären Sie sich damit einverstanden, die folgenden Informationen über das Kaspersky Security Center Linux an Kaspersky zu übertragen: die Version, die verwendete Lokalisierung, die ID der Softwarelizenz (d. h. die ID der Lizenz, die Sie verlängern) und ob Sie die Lizenz über ein Partnerunternehmen erworben haben oder nicht.

3. Folgen Sie im sich öffnenden Fensters des Dienstes für Lizenzverlängerung den Anweisungen um eine Lizenz zu verlängern.

   Die Lizenz wird verlängert.

In der Kaspersky Security Center Web Console werden die Benachrichtigungen für eine ablaufende Lizenz entsprechend des folgenden Zeitplans angezeigt:

- 30 Tage vor Ablauf
- 7 Tage vor Ablauf
- 3 Tage vor Ablauf
- 24 Stunden vor Ablauf
- Wenn eine Lizenz abgelaufen ist

Kaspersky Marketplace zum Finden von Kaspersky-Unternehmenslösungen verwenden

Der **Marketplace** ist ein Abschnitt im Hauptmenü, in dem Sie sich das gesamte Angebot an Unternehmenslösungen von Kaspersky anzeigen lassen können, die gewünschten auswählen und anschließend mit dem Kauf auf der Kaspersky-Website fortfahren können. Sie können Filter verwenden, um sich nur die Lösungen anzeigen zu lassen, die zu Ihrem Unternehmen und zu den Anforderungen an Ihr System für Informationssicherheit passen. Wenn Sie eine Lösung auswählen, leitet Sie Kaspersky Security Center Linux auf die entsprechende Webseite innerhalb der Kaspersky-Website weiter, wo Sie mehr über diese Lösung erfahren. Jede Produktseite ermöglicht es Ihnen, mit dem Kauf fortzufahren oder enthält Anweisungen zum Kaufprozess.

Im Abschnitt **Marketplace** können Sie die Lösungen von Kaspersky anhand der folgenden Kriterien filtern:

- Anzahl der Geräte (Endpunkte, Server und andere Arten von Assets), die Sie schützen möchten:
  - 50 – 250
  - 250-1000
  - Über 1000
- Entwicklungsstufe des Informationssicherheitsteams Ihres Unternehmens:
  - **Foundations**

    Diese Stufe ist typisch für Unternehmen, die nur über ein IT-Team verfügen. Die maximal mögliche Anzahl an Bedrohungen wird automatisch blockiert.
  - **Optimum**

    Diese Stufe ist typisch für Unternehmen, die eine bestimmte IT-Sicherheitsfunktion innerhalb des IT-Teams besitzen. Auf dieser Stufe benötigen Unternehmen Lösungen, die es ihnen ermöglichen, sich einfachen Bedrohungen, und Bedrohungen, die bestehende Präventionsmechanismen umgehen, entgegenzustellen.
  - **Expert**

    Diese Stufe ist typisch für Unternehmen mit komplexen und verteilten IT-Umgebungen. Das IT-Sicherheitsteam ist voll entwickelt oder das Unternehmen verfügt über ein eigenes SOC-Team (Security Operations Center). Die benötigten Lösungen ermöglichen es den Unternehmen, komplexen Bedrohungen und gezielten Angriffen zu begegnen.
- Zu schützende Arten von Assets:
  - **Endpunkte**: Workstations von Mitarbeitern, physische und virtuelle Maschinen, Embedded-Systeme
  - **Server**: physische und virtuelle Server
  - **Cloud**: öffentliche, private oder hybride Cloud-Umgebungen sowie Cloud-Dienste
  - **Netzwerk**: lokales Netzwerk, IT-Infrastruktur
  - **Service**: von Kaspersky angebotene sicherheitsbezogene Dienste

So finden und erwerben Sie eine Business-Lösung von Kaspersky:

1. Gehen Sie im Hauptfenster des Menüs zum **Marketplace**.

   Standardmäßig zeigt der Abschnitt alle verfügbaren Business-Lösungen von Kaspersky an.

2. Um nur die Lösungen anzuzeigen, die zu Ihrer Organisation passen, wählen Sie die erforderlichen Werte in den Filtern aus.

3. Klicken Sie auf die Lösung, die Sie kaufen möchten oder über die Sie mehr erfahren möchten.

Sie werden zur Webseite der Lösung weitergeleitet. Sie können den Anweisungen auf dem Bildschirm folgen, um mit dem Kauf fortzufahren.

Kaspersky-Anwendungen konfigurieren

Dieser Abschnitt enthält Informationen über die manuelle Konfiguration von Richtlinien und Aufgaben, über Benutzerrollen und über den Aufbau der Struktur der Administrationsgruppen und der Hierarchie von Aufgaben.

Szenario: Netzwerkschutz konfigurieren

Der Schnellstartassistent erstellt Richtlinien und Aufgaben mit den Standardeinstellungen. Es kann sein, dass diese Einstellungen nicht optimal sind oder in einem Unternehmen als verboten gelten. Es wird deshalb empfohlen, die Einstellungen dieser Richtlinien und Aufgaben zu optimieren, und anschließend erforderlichenfalls andere Richtlinien und Aufgaben für Ihr Netzwerk zu erstellen.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

- Kaspersky Security Center Linux Administrationsserver installiert haben
- Kaspersky Security Center Web Console installiert haben
- Das Hauptinstallationsszenario für Kaspersky Security Center Linux abgeschlossen haben
- Der Schnellstartassistent wurde abgeschlossen oder die folgenden Richtlinien und Aufgaben wurden manuell in der Administrationsgruppe **Verwaltete Geräte** erstellt:
  - Richtlinie von Kaspersky Endpoint Security
  - Gruppenaufgabe zum Update von Kaspersky Endpoint Security
  - Richtlinie für den Administrationsagenten
  - Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*

Schritte

Die Konfiguration des Netzwerkschutzes erfolgt schrittweise:

1. **Einrichtung und Verteilung von Richtlinien und Richtlinienprofilen für Kaspersky-Anwendungen**

   Zur Konfiguration und Verteilung der Einstellungen für auf den verwalteten Geräten installierte Kaspersky-Anwendungen stehen zwei unterschiedliche Methoden der Sicherheitsverwaltung zur Auswahl: die geräteorientierte und die benutzerorientierte Methode. Beide Methoden können kombiniert werden.

2. **Aufgaben zur Remote-Verwaltung von Kaspersky-Anwendungen konfigurieren**

   Überprüfen Sie die mit dem Schnellstartassistenten erstellten Aufgaben und passen Sie diese bei Bedarf noch feiner an.

   Vorgehensweisen: Gruppenaufgabe für das Update von Kaspersky Endpoint Security einrichten, Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates erstellen.

Erstellen Sie bei Bedarf zusätzliche Aufgaben, um die auf den Client-Geräten installierten Kaspersky-Anwendungen zu verwalten.

3. **Ereignismenge für Datenbank einschätzen und einschränken**

   Informationen über Ereignisse im Betrieb der verwalteten Anwendungen werden vom Client-Gerät übertragen und in der Administrationsserver-Datenbank registriert. Um die Belastung auf den Administrationsserver zu reduzieren, sollten Sie die maximale Anzahl der Ereignisse, die in der Datenbank gespeichert werden können, einschätzen und einschränken.

   Anleitung: Die Beschränkung der maximalen Anzahl der Ereignisse einstellen.

Ergebnisse

Nach Abschluss dieses Szenarios wird Ihr Netzwerk dank der Konfiguration von Kaspersky-Anwendungen, den Aufgaben und der vom Administrationsserver empfangenen Ereignissen geschützt sein.

- Die Kaspersky-Anwendungen werden entsprechend den Richtlinien und Richtlinienprofilen konfiguriert.
- Die Anwendungen werden über eine Reihe von Aufgaben verwaltet.
- Die maximale Anzahl der Ereignisse, die in der Datenbank gespeichert werden können, ist eingestellt.

Wenn der Netzwerkschutz angepasst ist, können Sie mit der Konfiguration von regelmäßigen Updates für die Datenbanken und Anwendungen von Kaspersky fortfahren.

Geräteorientierte und benutzerorientierte Methode der Sicherheitsverwaltung

Sie können die Sicherheitseinstellungen unter Berücksichtigung der Gerätefunktionen oder der Benutzerrollen verwalten. Die erste Methode wird *geräteorientierte Sicherheitsverwaltung* genannt, die zweite *benutzerorientierte Sicherheitsverwaltung*. Um verschiedene Programmeinstellungen auf verschiedene Geräte anzuwenden, können Sie eine dieser Verwaltungsmethoden oder eine Kombination aus beiden Methoden verwenden.

Mit der gerätezentrierten Sicherheitsverwaltung können Sie je nach gerätespezifischen Merkmalen unterschiedliche Einstellungen der Sicherheitsanwendung auf verwaltete Geräte anwenden. So können Sie beispielsweise Geräte, die in verschiedenen Administrationsgruppen zugeordnet sind, mit unterschiedlichen Einstellungen versehen.

Die benutzerorientierte Sicherheitsverwaltung ermöglicht es Ihnen, verschiedene Einstellungen der Sicherheitsanwendung auf verschiedene Benutzerrollen anzuwenden. Sie können mehrere Benutzerrollen anlegen, jedem Benutzer eine entsprechende Benutzerrolle zuweisen und verschiedene Anwendungseinstellungen für die Geräte definieren, die sich im Besitz von Benutzern mit unterschiedlichen Rollen befinden. So können Sie zum Beispiel den Geräten von Buchhaltern und den Geräten von Mitarbeitern der Personalabteilung unterschiedliche Anwendungseinstellungen zuweisen. Als Ergebnis erhält bei der benutzerorientierten Sicherheitsverwaltung jede Abteilung – die Buchhaltung und die Personalabteilung – eine eigene Konfiguration der Einstellungen für Kaspersky-Anwendungen. Die Konfiguration der Einstellungen legt fest, welche Anwendungseinstellungen von Benutzern angepasst werden können und welche zwangsweise übernommen und durch den Administrator gesperrt sind.

Bei der benutzerorientierten Sicherheitsverwaltung können Sie einzelnen Benutzern bestimmte Programmeinstellungen zuweisen. Das ist z. B. sinnvoll, wenn ein Mitarbeiter eine besondere Rolle im Unternehmen einnimmt oder wenn Sie Sicherheitsvorfälle überwachen möchten, die auf dem Gerät einer bestimmten Person auftreten. Unter Berücksichtigung der Rolle des Mitarbeiters im Unternehmen können Sie die Berechtigung dieser Person zur Änderung der Programmeinstellungen erweitern oder einschränken. So würden Sie z. B. die Berechtigungen eines Systemadministrators, der Client-Geräte im lokalen Büro verwaltet, erweitern.

Es ist auch eine Kombination der geräteorientierten und der benutzerorientierten Herangehensweise an die Sicherheitsverwaltung möglich. So können Sie zum Beispiel für jede Administrationsgruppe eine bestimmte Anwendungsrichtlinie anpassen und Richtlinienprofile für eine oder mehrere Benutzerrollen Ihres Unternehmens erstellen. In diesem Fall werden die Richtlinien und Richtlinienprofile in der folgenden Reihenfolge angewendet:

1. Es werden Richtlinien angewendet, die für geräteorientierte Sicherheitsverwaltung erstellt wurden.
2. Sie werden mittels Richtlinienprofilen gemäß den Prioritäten der Profile geändert.
3. Die Richtlinien werden von den Richtlinienprofilen geändert, die Benutzerrollen zugewiesen sind.

Richtlinien einrichten und verwalten: geräteorientierte Herangehensweise

Nach Abschluss dieses Szenarios werden die Anwendungen gemäß den von Ihnen festgelegten Richtlinien und Richtlinienprofilen auf allen verwalteten Geräten konfiguriert.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie den Kaspersky Security Center Linux Administrationsserver und Kaspersky Security Center Web Console installiert haben. Sie sollten zusätzlich auch die benutzerorientierte Sicherheitsverwaltung als Alternative oder als zusätzliche Option zur geräteorientierten Herangehensweise in Betracht ziehen. Weitere Informationen über beiden Verwaltungsmethoden.

Schritte

Das Szenario der geräteorientierten Verwaltung der Kaspersky-Anwendungen umfasst die folgenden Schritte:

1. **Anwendungsrichtlinien anpassen**

   Passen Sie die Einstellungen der auf den verwalteten Geräten installierten Kaspersky-Anwendungen an, indem Sie für jede Anwendung eine Richtlinie erstellen. Diese Auswahl an Richtlinien wird an die Client-Geräte weitergegeben.

   Wenn Sie den Schutz Ihres Netzwerks im Schnellstartassistenten konfigurieren, erstellt Kaspersky Security Center Linux eine Standardrichtlinie für die folgenden Anwendungen:

   - Kaspersky Endpoint Security für Linux – für Linux-basierte Client-Geräte
   - Kaspersky Endpoint Security für Windows – für Windows-basierte Client-Geräte

   Wenn Sie den Konfigurationsvorgang mithilfe dieses Assistenten abgeschlossen haben, müssen Sie keine neue Richtlinie für diese Anwendung erstellen.

Wenn Sie eine hierarchische Struktur aus mehreren Administrationsservern und/oder Administrationsgruppen haben, erben die sekundären Administrationsserver und die untergeordneten Administrationsgruppen standardmäßig die Richtlinien des primären Administrationsservers. Sie können die Vererbung an die untergeordneten Gruppen und an den sekundären Administrationsserver erzwingen, um Änderungen an den durch die Richtlinie höherer Ebene festgelegten Einstellungen zu verhindern. Wenn Sie möchten, dass nur bestimmte Einstellungen zwangsweise vererbt werden, können Sie diese in der Richtlinie höherer Ebene sperren. Die übrigen, nicht gesperrten Einstellungen können in den Richtlinien niedriger Ebene geändert werden. Dank der erstellten Hierarchie aus Richtlinien können Sie die Geräte in den Administrationsgruppen optimal verwalten.

Anleitung: Richtlinie erstellen

2. **Richtlinienprofile erstellen (optional)**

   Wenn Sie möchten, dass Geräte innerhalb einer Administrationsgruppe verschiedene Richtlinieneinstellungen erhalten, erstellen Sie Richtlinienprofile für diese Geräte. Ein Richtlinienprofil ist eine benannte Teilmenge von Richtlinieneinstellungen. Diese Teilmenge wird auf Zielgeräten gemeinsam mit der Richtlinie verteilt und ergänzt sie unter einer bestimmten Bedingung, die als *Profilaktivierungsbedingung* bezeichnet wird. Profile enthalten nur jene Einstellungen, die sich von der "zugrundeliegenden" Richtlinie unterscheiden, die auf dem verwalteten Gerät aktiv ist.

   Die Verwendung von Bedingungen zur Aktivierung von Profilen erlaubt es, verschiedene Richtlinienprofile auf Geräte anzuwenden, die eine bestimmte Hardware-Konfiguration besitzen oder mit bestimmten Tags markiert sind. Verwenden Sie Tags, um Geräte anhand bestimmter Kriterien zu filtern. So können Sie z. B. das Tag *CentOS* erstellen, es allen Geräten mit einem CentOS-Betriebssystem zuweisen und dieses Tag dann als Bedingung zur Aktivierung eines Richtlinienprofils festlegen. Als Ergebnis werden alle Kaspersky-Anwendungen, die auf CentOS-Geräten installiert sind, von ihrem eigenen Richtlinienprofil verwaltet.

   Anleitung:

   - Richtlinienprofil erstellen
   - Regeln für die Aktivierung des Richtlinienprofils erstellen

3. **Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergeben**

   Standardmäßig wird der Administrationsserver alle 15 Minuten automatisch mit den verwalteten Geräten synchronisiert. Während der Synchronisierung werden neue oder veränderte Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergegeben. Sie können die automatische Synchronisierung umgehen und die Synchronisierung auch manuell mit dem Befehl Synchronisierung erzwingen ausführen. Sobald die Synchronisierung abgeschlossen ist, werden die Richtlinien und Richtlinienprofile an die installierten Kaspersky-Anwendungen weitergegeben und von ihnen übernommen.

   Sie können überprüfen, ob die Richtlinien und Richtlinienprofile an ein bestimmtes Gerät übertragen wurden. Kaspersky Security Center Linux registriert das Datum und die Uhrzeit der Weitergabe in den Eigenschaften des Geräts.

   Anleitung: Erzwungene Synchronisierung

Ergebnisse

Nach Abschluss des geräteorientierten Szenarios werden die Kaspersky-Anwendungen gemäß den festgelegten Einstellungen konfiguriert und mittels Richtlinienhierarchie weitergegeben.

Die konfigurierten Anwendungsrichtlinien und Richtlinienprofile werden automatisch auf neue Geräte angewendet, die zu den Administrationsgruppen hinzugefügt werden.

Richtlinien einrichten und verwalten: benutzerorientierte Herangehensweise

Dieser Abschnitt beschreibt das Szenario der benutzerorientierten Herangehensweise an die zentralisierte Konfiguration der Kaspersky-Anwendungen, die auf den verwalteten Geräten installiert sind. Nach Abschluss dieses Szenarios werden die Programme gemäß den von Ihnen festgelegten Richtlinien und Richtlinienprofilen auf allen verwalteten Geräten konfiguriert.

Erforderliche Vorrausetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie den Kaspersky Security Center Linux Administrationsserver und Kaspersky Security Center Web Console erfolgreich installiert und das Hauptbereitstellungsszenario abgeschlossen haben. Sie sollten zusätzlich auch die geräteorientierte Sicherheitsverwaltung als Alternative oder als zusätzliche Option zur benutzerorientierten Herangehensweise in Betracht ziehen. Weitere Informationen über beiden Verwaltungsmethoden.

Prozess

Das Szenario der benutzerorientierten Verwaltung der Kaspersky-Anwendungen umfasst die folgenden Schritte:

1. **Programmrichtlinien anpassen**

   Passen Sie die Einstellungen der auf den verwalteten Geräten installierten Kaspersky-Anwendungen an, indem Sie für jede Anwendung eine Richtlinie erstellen. Diese Auswahl an Richtlinien wird an die Client-Geräte weitergegeben.

   Wenn Sie den Schutz Ihres Netzwerks im Schnellstartassistenten konfigurieren, erstellt Kaspersky Security Center Linux eine Standardrichtlinie für Kaspersky Endpoint Security. Wenn Sie den Konfigurationsvorgang mithilfe dieses Assistenten abgeschlossen haben, müssen Sie keine neue Richtlinie für dieses Programm erstellen.

   Wenn Sie eine hierarchische Struktur aus mehreren Administrationsservern und/oder Administrationsgruppen haben, erben die sekundären Administrationsserver und die untergeordneten Administrationsgruppen standardmäßig die Richtlinien des primären Administrationsservers. Sie können die Vererbung an die untergeordneten Gruppen und an den sekundären Administrationsserver erzwingen, um Änderungen an den durch die Richtlinie höherer Ebene festgelegten Einstellungen zu verhindern. Wenn Sie möchten, dass nur bestimmte Einstellungen zwangsweise vererbt werden, können Sie diese in der Richtlinie höherer Ebene sperren. Die übrigen, nicht gesperrten Einstellungen können in den Richtlinien niedriger Ebene geändert werden. Dank der erstellten Hierarchie aus Richtlinien können Sie die Geräte in den Administrationsgruppen optimal verwalten.

   Anleitung: Richtlinie erstellen

2. **Gerätebenutzer angeben**

   Weisen Sie die verwalteten Geräte den entsprechenden Benutzern zu.

   Anleitung: Festlegen eines Benutzers als Gerätebesitzer

3. **Typische Benutzerrollen in Ihrem Unternehmen festlegen**

   Überlegen Sie, in welchen unterschiedlichen Bereichen die Mitarbeiter Ihres Unternehmens tätig sind. Teilen Sie alle Mitarbeiter nach ihren Rollen ein. Sie können sie z. B. nach Abteilungen, Berufen oder Positionen unterteilen. Anschließend müssen Sie für jede Gruppe eine Benutzerrolle erstellen. Bedenken Sie, dass jede Benutzerrolle ihr eigenes Richtlinienprofil mit rollenspezifischen Anwendungseinstellungen erhält.

4. **Benutzerrollen erstellen**

   Erstellen und konfigurieren Sie eine Benutzerrolle für jede der Mitarbeitergruppen, die Sie im vorherigen Schritt festgelegt haben, oder verwenden Sie vorkonfigurierte Benutzerrollen. Die Benutzerrollen enthalten eine Auswahl an Zugriffsrechten für Anwendungsfunktionen.

   Anleitung: Benutzerrolle erstellen

5. **Umfang jeder Benutzerrolle festlegen**

   Geben Sie für jede erstellte Benutzerrolle die Benutzer und/oder die Sicherheitsgruppen und Administrationsgruppen an. Einstellungen, die mit einer Benutzerrolle verbunden sind, gelten nur für Geräte, die Benutzern gehören, die über diese Rolle verfügen, und nur, wenn diese Geräte zu Gruppen gehören, die mit dieser Rolle verbunden sind, einschließlich untergeordnete Gruppen.

   Anleitung: Bearbeiten des Bereichs einer Benutzerrolle

6. **Richtlinienprofile erstellen**

   Erstellen Sie für jede Benutzerrolle in Ihrem Unternehmen ein Richtlinienprofil. Die Richtlinienprofile bestimmen, welche Einstellungen für die auf den Benutzergeräten installierten Anwendungen gelten, wobei die Rolle jedes Benutzers berücksichtigt wird.

   Anleitung: Richtlinienprofil erstellen

7. **Richtlinienprofile mit Benutzerrollen verbinden**

   Verbinden Sie die erstellten Richtlinienprofile mit den Benutzerrollen. Das Richtlinienprofil gilt dann für Benutzer mit der festgelegten Rolle. Die im Richtlinienprofil angepassten Einstellungen werden auf Kaspersky-Anwendungen angewendet, die auf den Benutzergeräten installiert sind.

   Anleitung: Verbinden von Richtlinienprofilen mit Rollen

8. **Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergeben**

   Standardmäßig synchronisiert Kaspersky Security Center Linux den Administrationsserver automatisch alle 15 Minuten mit den verwalteten Geräten. Während der Synchronisierung werden neue oder veränderte Richtlinien und Richtlinienprofile an die verwalteten Geräte weitergegeben. Sie können die automatische Synchronisierung umgehen und die Synchronisierung auch manuell mit dem Befehl Synchronisierung erzwingen ausführen. Sobald die Synchronisierung abgeschlossen ist, werden die Richtlinien und Richtlinienprofile an die installierten Kaspersky-Anwendungen weitergegeben und von ihnen übernommen.

   Sie können überprüfen, ob die Richtlinien und Richtlinienprofile an ein bestimmtes Gerät übertragen wurden. Kaspersky Security Center Linux registriert das Datum und die Uhrzeit der Weitergabe in den Eigenschaften des Geräts.

   Anleitung: Erzwungene Synchronisierung

Ergebnisse

Nach Abschluss des benutzerorientierten Szenarios werden die Kaspersky-Anwendungen gemäß den festgelegten Einstellungen konfiguriert und mittels der Hierarchie von Richtlinien und Richtlinienprofilen weitergegeben.

Für einen neuen Benutzer muss ein neues Benutzerkonto erstellt werden. Anschließend müssen dem Benutzer eine der erstellten Benutzerrollen sowie Geräte zugewiesen werden. Die konfigurierten Anwendungsrichtlinien und Richtlinienprofile werden automatisch auf die Geräte dieses Benutzers angewendet.

Richtlinien und Richtlinienprofile

In Kaspersky Security Center Web Console können Sie Richtlinien für Kaspersky-Anwendungen erstellen. In diesem Abschnitt werden Richtlinien und Richtlinienprofile beschrieben, und Sie erhalten Anweisungen für deren Erstellung und Änderung.

Über Richtlinien und Richtlinienprofile

Eine *Richtlinie* besteht aus einer Reihe von Einstellungen für eine Kaspersky-Anwendung, die auf eine Administrationsgruppe und deren Untergruppen angewendet werden. Sie können mehrere Kaspersky-Anwendungen auf den Geräten einer Administrationsgruppe installieren. Kaspersky Security Center bietet eine einzelne Richtlinie für jede Kaspersky-Anwendung in einer Administrationsgruppe. Eine Richtlinie hat eine der folgenden Statusvarianten:

Status der Richtlinie

Status	Beschreibung
Aktiv	Die aktuelle Richtlinie, die auf das Gerät angewendet wird. In jeder Administrationsgruppe kann nur eine Richtlinie für eine Kaspersky-Anwendung aktiv sein. Geräte wenden die Einstellungswerte einer aktiven Richtlinie für eine Kaspersky-Anwendung an.
Inaktiv	Eine Richtlinie, die derzeit nicht auf ein Gerät angewendet wird.
Für mobile Benutzer	Bei Auswahl dieser Option wird die Richtlinie aktiv, sobald das Gerät vom Unternehmensnetzwerk getrennt wird.

Richtlinien funktionieren gemäß den folgenden Regeln:

- Für eine einzelne Anwendung können mehrere Richtlinien mit unterschiedlichen Werten konfiguriert werden.
- Für die aktuelle Anwendung kann nur eine Richtlinie aktiv sein.
- Eine Richtlinie kann untergeordnete Richtlinien haben.

Im Allgemeinen können Sie Richtlinien als Vorbereitung für Notfallsituationen wie Virenangriffe verwenden. Beispiel: Wenn ein Angriff über Flash-Laufwerke erfolgt, können Sie eine Richtlinie aktivieren, die den Zugriff auf Flash-Laufwerke blockiert. In diesem Fall wird die aktuell aktive Richtlinie automatisch inaktiv.

Um zu verhindern, dass mehrere Richtlinien verwaltet werden, können Sie beispielsweise Richtlinienprofile verwenden, wenn bei verschiedenen Gelegenheiten nur bestimmte Einstellungen geändert werden müssen.

Ein *Richtlinienprofil* stellt eine benannte Teilmenge von Einstellungswerten einer Richtlinie dar, welche die Einstellungswerte in einer Richtlinie ersetzen. Ein Richtlinienprofil wirkt sich auf die effektive Formation der Einstellungen auf einem verwalteten Gerät aus. *Effektive Einstellungen* stellen eine Zusammenstellung an Einstellungen für Richtlinien, Richtlinienprofile und lokalen Anwendungseinstellungen dar, die derzeit für das Gerät angewendet werden.

Richtlinienprofile funktionieren entsprechend den folgenden Regeln:

- Ein Richtlinienprofil wird wirksam, wenn eine bestimmte Aktivierungsbedingung erfüllt ist.
- Richtlinienprofile enthalten Werte für Einstellungen, die von den Richtlinieneinstellungen abweichen.

- Durch das Aktivieren eines Richtlinienprofils werden die effektiven Einstellungen des verwalteten Gerätes geändert.
- Eine Richtlinie kann nicht mehr als 100 Richtlinienprofile enthalten.

Über das Schloss und gesperrte Einstellungen

Jede Richtlinieneinstellung verfügt über eine Schaltfläche mit einem Sperren-Symbol (🔒). Die folgende Tabelle zeigt die Statuswerte der Schaltflächen zum Sperren an:

Status der Sperrschaltfläche

Status	Beschreibung
Undefined	Wenn neben einer Einstellung eine offene Sperre angezeigt wird und die Umschalttaste deaktiviert ist, wird die Einstellung in der Richtlinie nicht angegeben. Ein Benutzer kann diese Einstellungen in der Oberfläche der verwalteten Anwendung ändern. Diese Art von Einstellungen wird als *entsperrt* bezeichnet.
Enforce	Wenn neben einer Einstellung eine Sperre angezeigt wird und die Umschalttaste aktiviert ist, wird die Einstellung auf die Geräte angewendet, auf denen die Richtlinie erzwungen wird. Ein Benutzer kann die Werte dieser Einstellungen in Oberfläche einer verwalteten Anwendung nicht ändern. Diese Art von Einstellungen wird als *gesperrt* bezeichnet.

Es wird dringend empfohlen, dass Sie für Richtlinieneinstellungen, die Sie auf verwalteten Geräten anwenden möchten, die Sperre aktivieren. Nicht gesperrte Richtlinieneinstellungen können in den Einstellungen der Kaspersky-Anwendungen auf verwalteten Geräten geändert werden.

Sie können eine Sperrschaltfläche verwenden, um die folgenden Aktionen auszuführen:

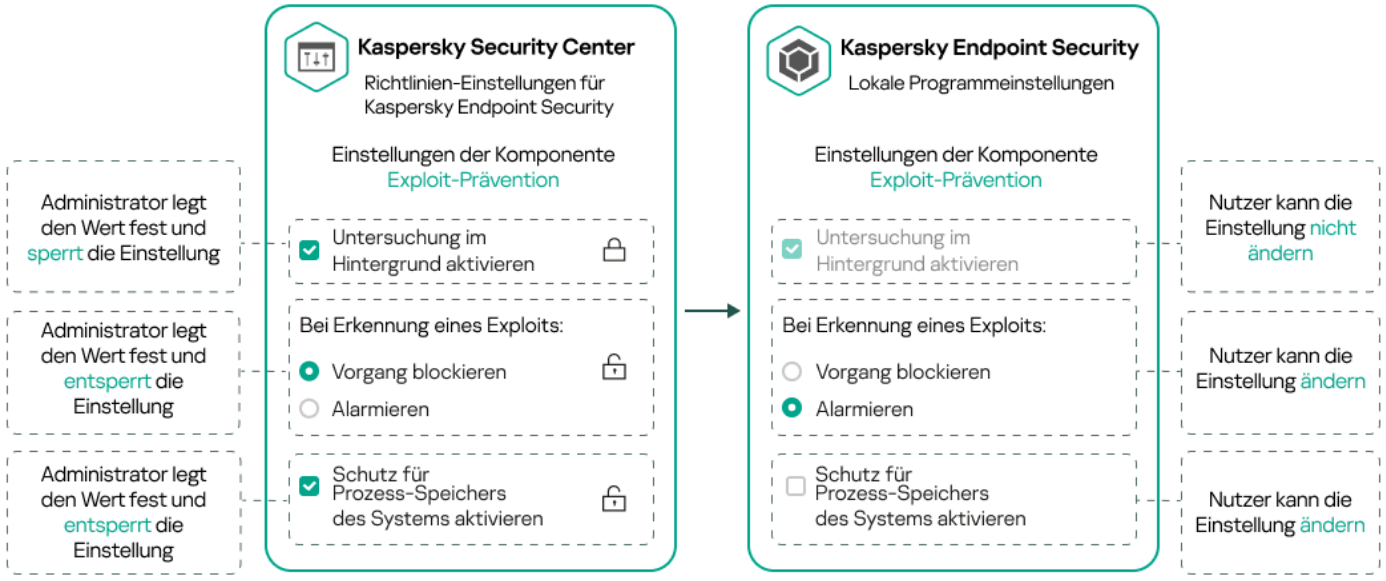
- Sperren von Einstellungen für eine Verwaltungsuntergruppenrichtlinie
- Sperren von Einstellungen einer Kaspersky-Anwendung auf einem verwalteten Gerät

Eine gesperrte Einstellung wird zum Implementieren effektiver Einstellungen auf einem verwalteten Gerät verwendet.

Ein Vorgang zum effektiven Implementieren von Einstellungen umfasst die folgenden Aktionen:

- Das verwaltete Gerät wendet die Einstellungswerte der Kaspersky-Anwendung an.
- Das verwaltete Gerät wendet gesperrte Einstellungswerte einer Richtlinie an.

Eine Richtlinie und eine verwaltete Kaspersky-Anwendung enthalten dieselben Einstellungen. Wenn Sie Richtlinieneinstellungen konfigurieren, ändern die Einstellungen der Kaspersky-Anwendung die Werte auf einem verwalteten Gerät. Sie können gesperrte Einstellungen auf einem verwalteten Gerät nicht anpassen (siehe Abbildung unten):



Sperren und Einstellungen der Kaspersky-Anwendungen

Vererbung von Richtlinien und Richtlinienprofilen

Dieser Abschnitt enthält Informationen zur Hierarchie und Vererbung von Richtlinien und Richtlinienprofilen.

Hierarchie der Richtlinien

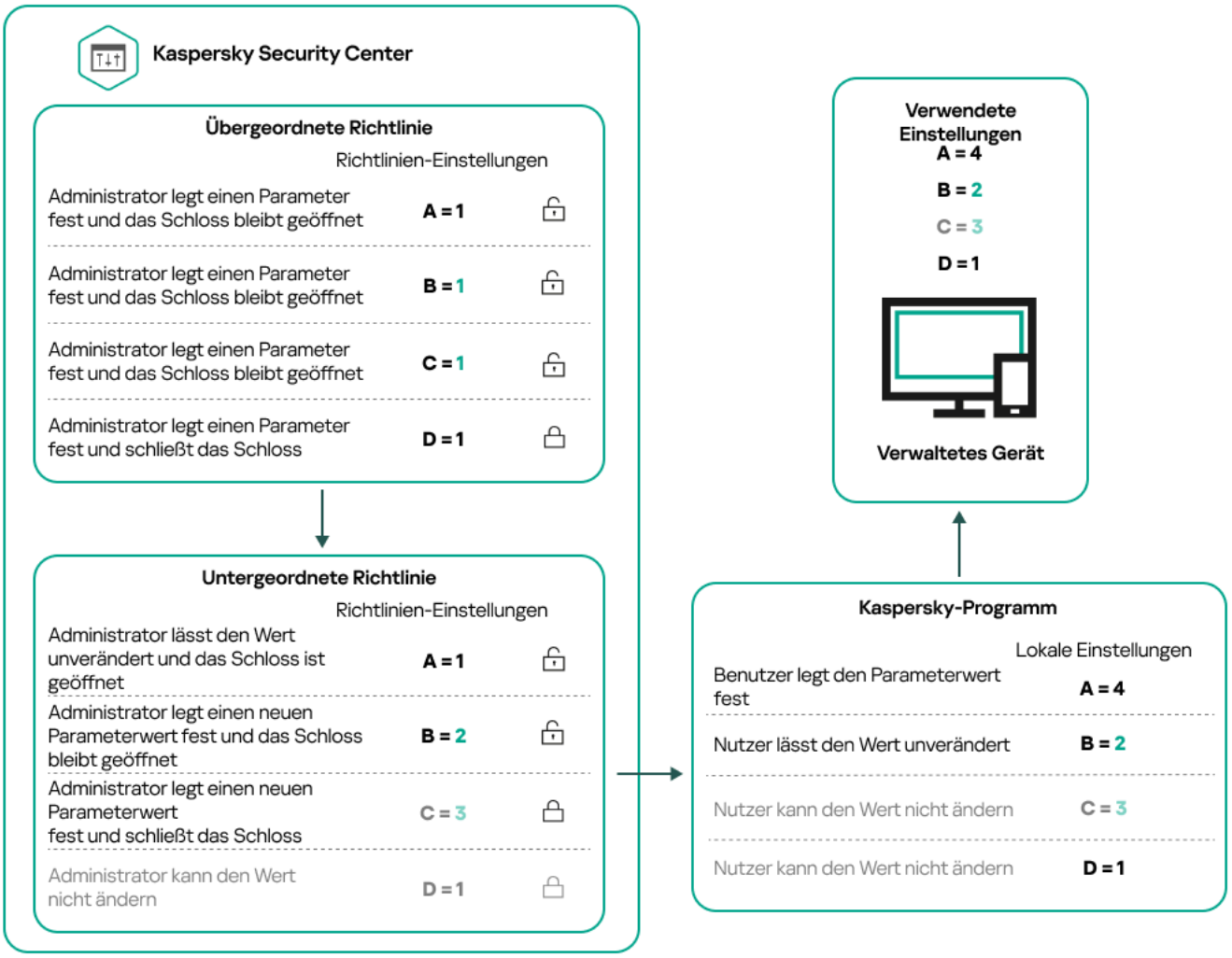
Wenn unterschiedliche Geräte unterschiedliche Einstellungen benötigen, können Sie Geräte in Administrationsgruppen organisieren.

Sie können eine Richtlinie für eine einzelne Administrationsgruppe angeben. Richtlinieneinstellungen können *vererbt* werden. Vererbung bedeutet, dass Richtlinieneinstellungswerte in Untergruppen (untergeordneten Gruppen) von einer Richtlinie einer übergeordneten Administrationsgruppe empfangen werden.

Im Weiteren wird eine Richtlinie für eine übergeordnete Gruppe auch als *übergeordnete Richtlinie* bezeichnet. Eine Richtlinie für eine Untergruppe (untergeordnete Gruppe) wird auch als *untergeordnete Richtlinie* bezeichnet.

Standardmäßig ist auf dem Administrationsserver mindestens eine Gruppe mit verwalteten Geräten vorhanden. Wenn Sie benutzerdefinierte Gruppen erstellen möchten, werden diese als Untergruppen (untergeordnete Gruppen) innerhalb der Gruppe mit verwalteten Geräten erstellt.

Richtlinien derselben Anwendung wirken gemäß einer Hierarchie von Verwaltungsgruppen aufeinander ein. Gesperrte Einstellungen aus einer Richtlinie einer übergeordneten Administrationsgruppe weisen die Richtlinieneinstellungswerte einer Untergruppe neu zu (siehe Abbildung unten).

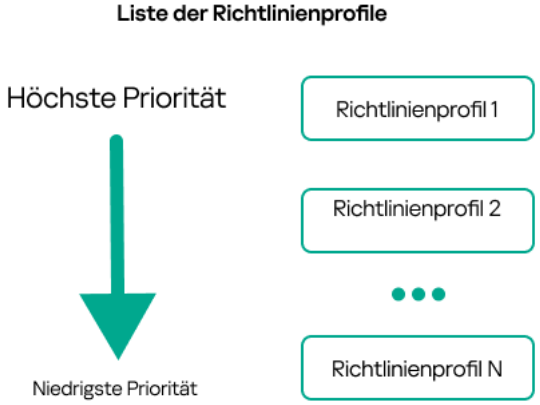


Hierarchie der Richtlinien

Richtlinienprofile in einer Hierarchie von Richtlinien

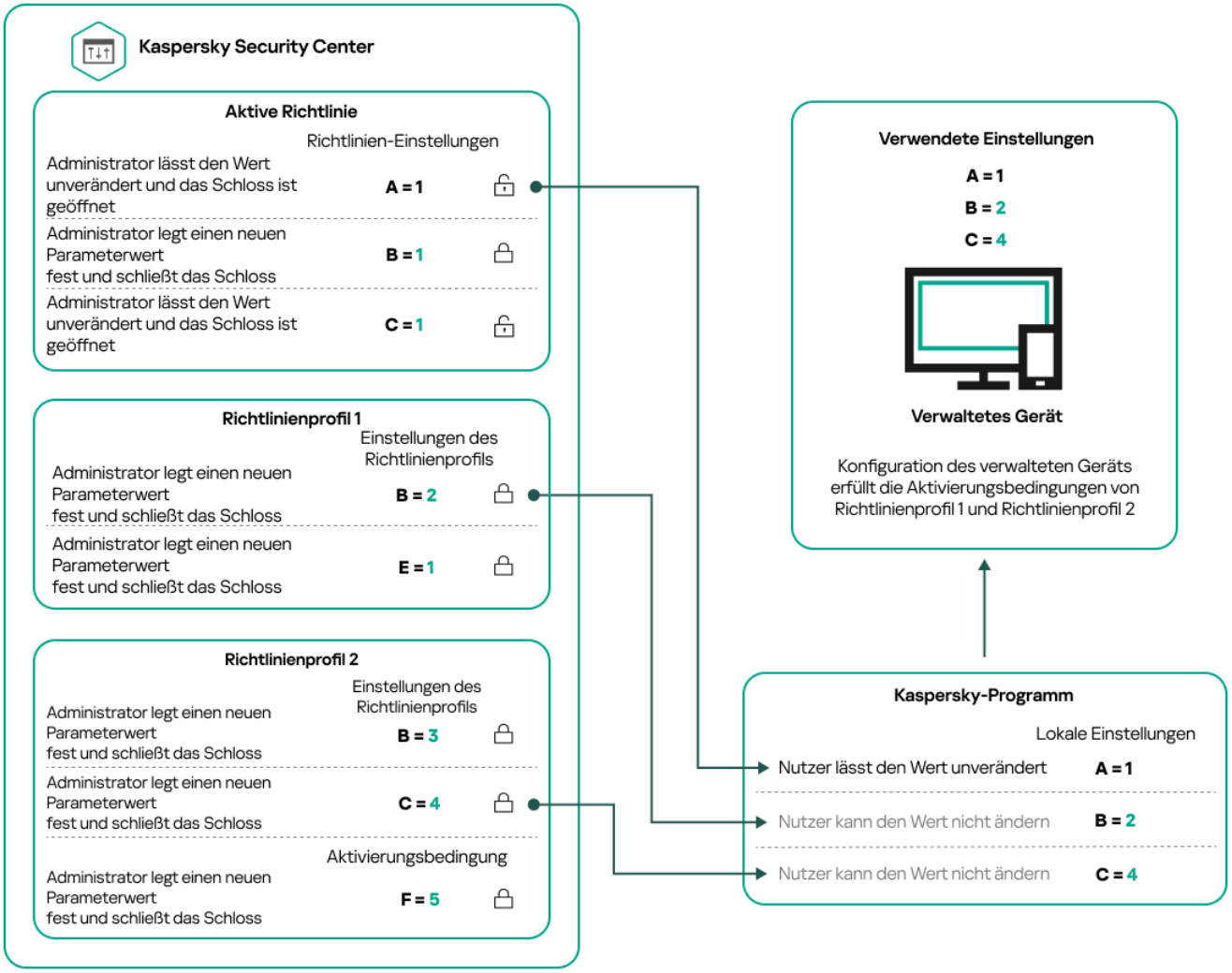
Richtlinienprofile haben die folgenden Bedingungen für die Prioritätszuweisung:

- Die Position eines Profils in einer Richtlinienprofilliste gibt seine Priorität an. Die Priorität eines Richtlinienprofils kann geändert werden. Die höchste Position in einer Liste gibt die höchste Priorität an (siehe Abbildung unten).



Prioritätsdefinition eines Richtlinienprofils

- Die Aktivierungsbedingungen von Richtlinienprofilen hängen nicht voneinander ab. Es können mehrere Richtlinienprofile gleichzeitig aktiviert werden. Wenn sich mehrere Richtlinienprofile auf dieselbe Einstellung auswirken, übernimmt das Gerät den Einstellungswert aus dem Richtlinienprofil mit der höchsten Priorität (siehe Abbildung unten).



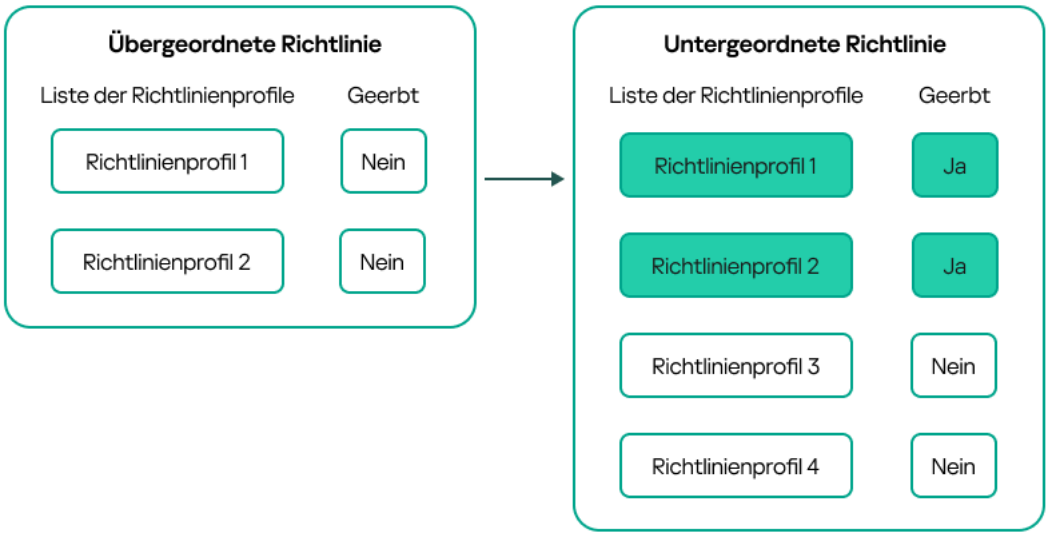
Die Konfiguration des verwalteten Geräts erfüllt die Aktivierungsbedingungen mehrerer Richtlinienprofile.

Richtlinienprofile in einer Vererbungshierarchie

Richtlinienprofile aus verschiedenen Richtlinien auf Hierarchieebene erfüllen die folgenden Bedingungen:

- Eine Richtlinie auf niedrigerer Ebene erbt Richtlinienprofile von einer Richtlinie auf höherer Ebene. Ein Richtlinienprofil, das von einer übergeordneten Richtlinie geerbt wurde, erhält eine höhere Priorität als die Ebene des ursprünglichen Richtlinienprofils.

- Die Priorität eines geerbten Richtlinienprofils kann nicht geändert werden (siehe Abbildung unten).



Vererbung von Richtlinienprofilen

Richtlinienprofile mit demselben Namen

Wenn zwei Richtlinien mit demselben Namen in unterschiedlichen Hierarchieebenen vorhanden sind, funktionieren diese Richtlinien gemäß den folgenden Regeln:

- Gesperrte Einstellungen und die Profilaktivierungsbedingung eines übergeordneten Richtlinienprofils ändern die Einstellungen und die Profilaktivierungsbedingung eines untergeordneten Richtlinienprofils (siehe Abbildung unten).



Das untergeordnete Profil erbt Einstellungswerte von einem übergeordneten Richtlinienprofil.

- Entsperrte Einstellungen und die Profilaktivierungsbedingung eines übergeordneten Richtlinienprofils ändern nicht die Einstellungen und die Profilaktivierungsbedingung eines untergeordneten Richtlinienprofils.

Implementierung der Einstellungen auf einem verwalteten Gerät

Die Implementierung von effektiven Einstellungen auf einem verwalteten Gerät kann wie folgt beschrieben werden:

- Die Werte aller Einstellungen, die nicht gesperrt wurden, werden aus der Richtlinie übernommen.
- Anschließend werden sie mit den Einstellungswerten der verwalteten Anwendung überschrieben.
- Anschließend werden die gesperrten Einstellungswerte aus der effektiven Richtlinie angewendet. Die Werte gesperrter Einstellungen ändern die Werte nicht gesperrter effektiver Einstellungen.

Richtlinien verwalten

Dieser Abschnitt beschreibt das Verwalten von Richtlinien und enthält Informationen zum Anzeigen der Richtlinienliste, zum Erstellen einer Richtlinie, zum Ändern einer Richtlinie, zum Kopieren einer Richtlinie, zum Verschieben einer Richtlinie, zum erzwungenen Synchronisieren, zum Anzeigen des Statusdiagramms für die Richtlinienverteilung und zum Löschen einer Richtlinie.

Richtlinienliste anzeigen

Sie können die Richtlinienlisten für den Administrationsserver oder für jede beliebige Administrationsgruppe anzeigen.

Um sich die Richtlinienliste anzeigen zu lassen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Gruppenhierarchie**.

2. Wählen Sie in der Struktur der Administrationsgruppe die Administrationsgruppe aus, für welche Sie die Liste mit Richtlinien anzeigen möchten.

   Daraufhin wird die Liste der Richtlinien in Tabellenformat geöffnet. Wenn noch keine Richtlinien existieren, ist die Tabelle leer. Sie können die Spalten der Tabelle ein- und ausblenden, ihre Reihenfolge verändern, nur Zeilen mit einem bestimmten Wert anzeigen und die Suchfunktion verwenden.

Richtlinie erstellen

Sie können Richtlinien erstellen sowie Sie bestehende Richtlinien ändern und löschen.

Um eine Richtlinie zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

2. Wählen Sie die Administrationsgruppe aus, für welche die Richtlinie erstellt werden soll:

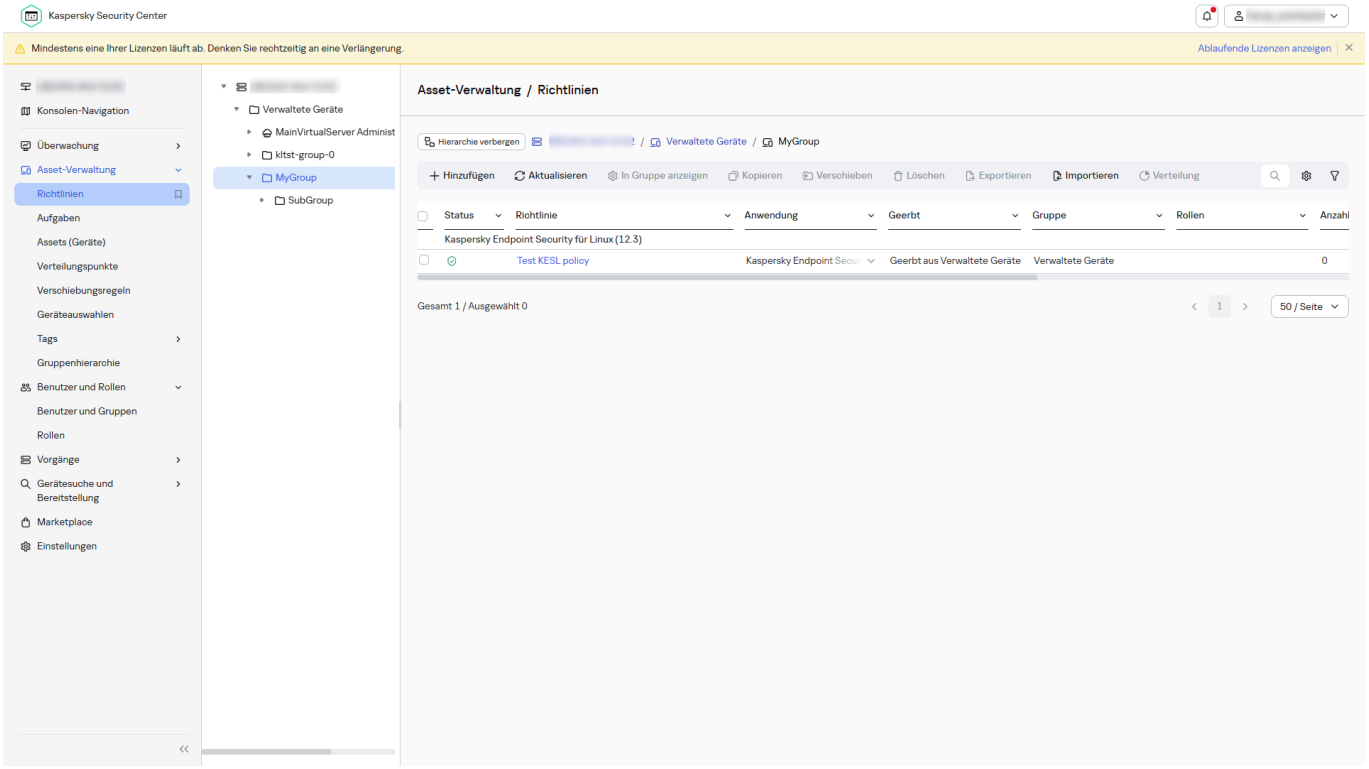
   - Für die Stammgruppe:
     In diesem Fall können Sie mit dem nächsten Schritt fortfahren.

   - Für eine untergeordnete Gruppe:

     a. Klicken Sie im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**.
        Der Name der Schaltfläche ändert sich zu **Hierarchie verbergen**.

     b. Klicken Sie im neuen Fenster auf den Namen der erforderlichen Untergruppe.

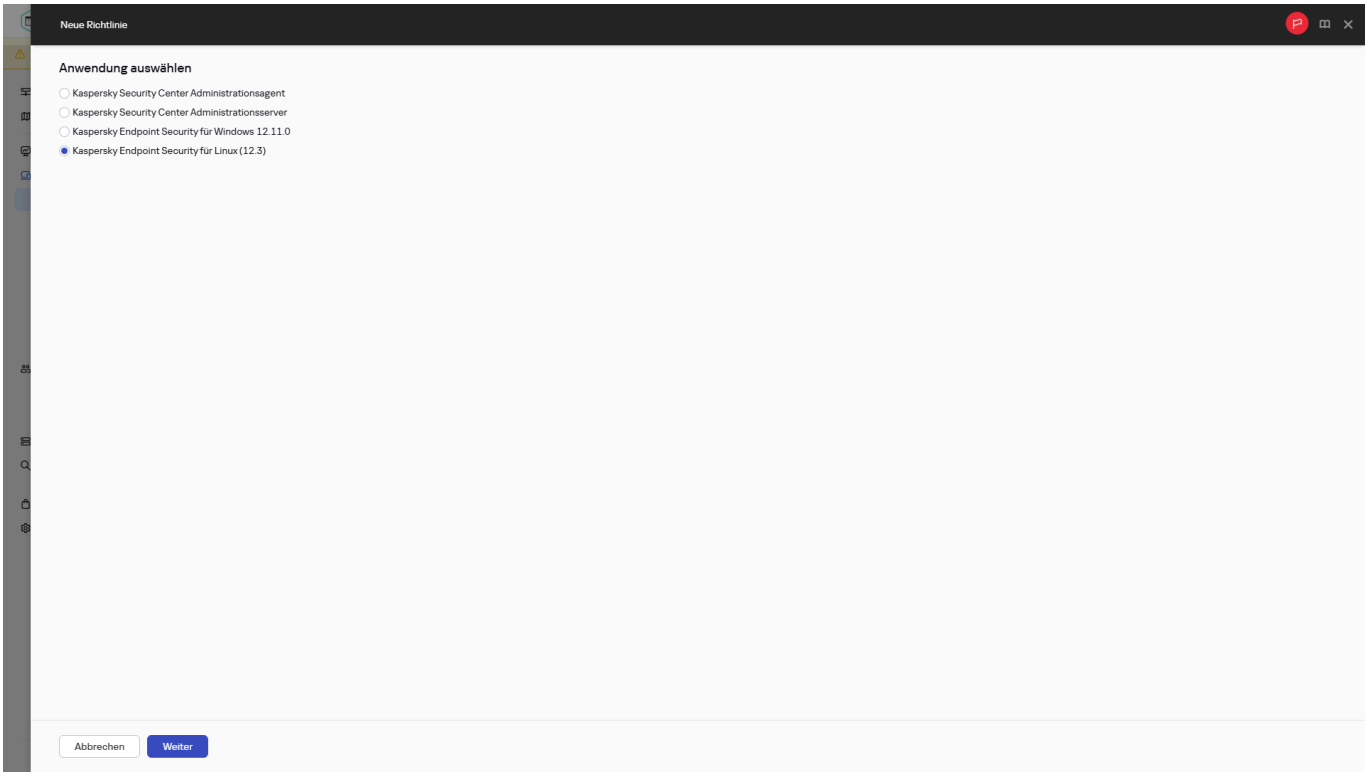
Der Pfad zur ausgewählten Gruppe wird im oben Bereich der Seite angezeigt. Bei Bedarf können Sie auf einen Link mit dem Namen der Administrationsgruppe klicken, um zu dieser Gruppe zu gelangen. Der letzte Link im Pfad ist standardmäßig inaktiv. Außerdem können Sie das Hierarchiefenster schließen, indem Sie auf die Schaltfläche **Hierarchie verbergen** klicken.



Die Liste der Richtlinien

3. Klicken Sie auf die Schaltfläche **Hinzufügen**.

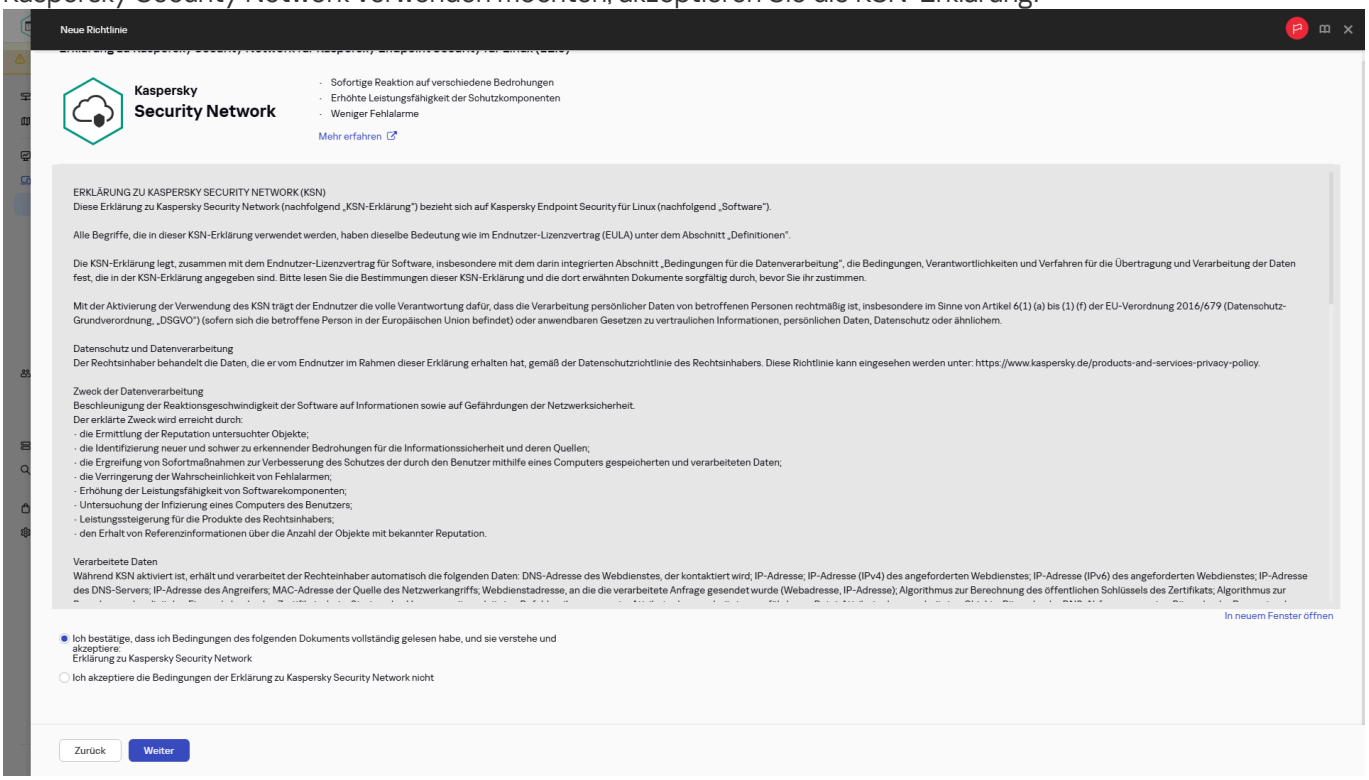
   Das Fenster **Anwendung auswählen** wird geöffnet.



Eine neue Richtlinie erstellen

4. Wählen Sie die Anwendung aus, für das Sie eine Richtlinie erstellen möchten.

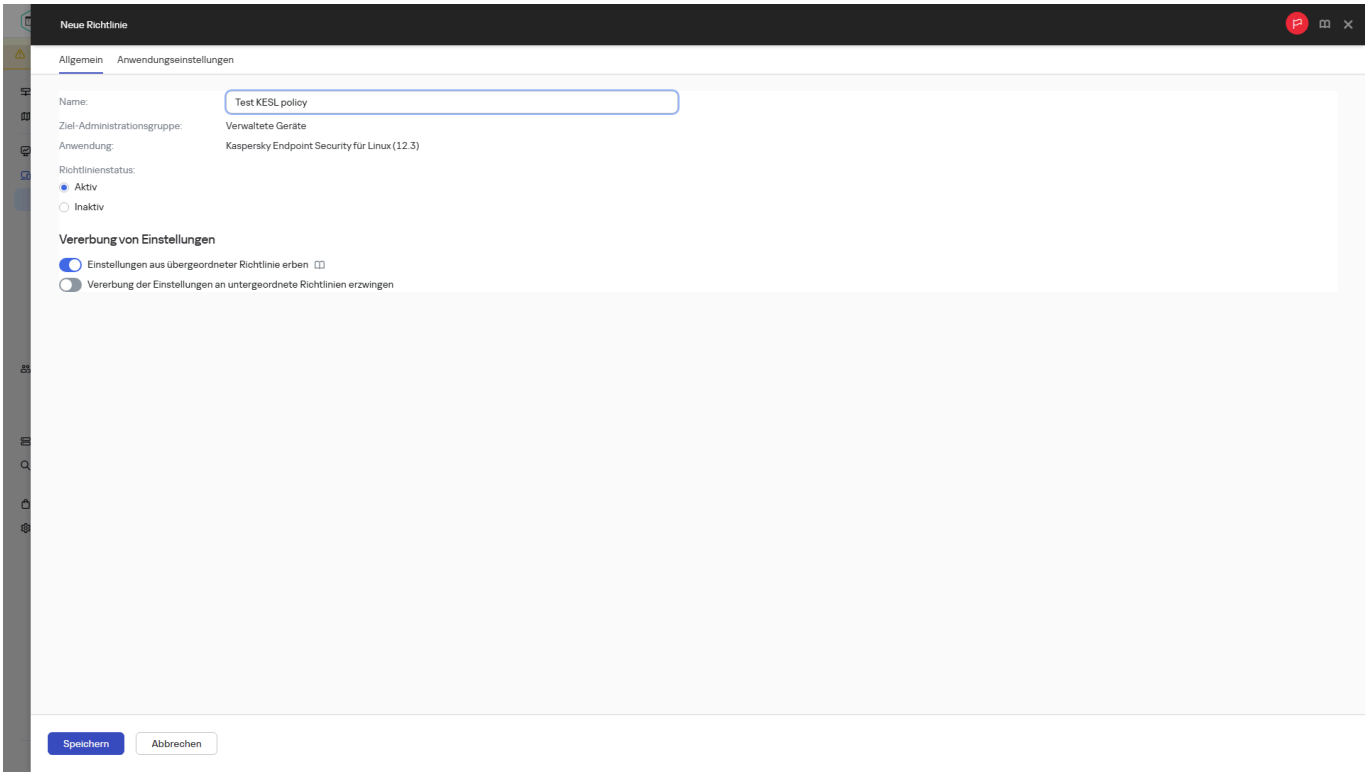
5. Wenn die Anwendung, für die Sie die Richtlinie erstellen möchten, die Verwendung von Kaspersky Security Network unterstützt, werden Sie aufgefordert, die KSN-Erklärung zu akzeptieren Wenn Sie Kaspersky Security Network verwenden möchten, akzeptieren Sie die KSN-Erklärung.



Akzeptieren der KSN-Erklärung

6. Klicken Sie auf die Schaltfläche **Weiter**.

   Das Fenster für neue Richtlinieneinstellungen wird geöffnet, in dem die Registerkarte **Allgemein** ausgewählt ist. Ändern Sie gegebenenfalls Standardname, Standardstatus und Standardvererbungseinstellungen der Richtlinie.



Das Fenster mit den Einstellungen der neuen Richtlinie

7. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

Sie können aber auch auf **Speichern** klicken und beenden. Die Richtlinie wird in der Liste der Richtlinien angezeigt, und Sie können ihre Einstellungen später anpassen.

8. Wählen Sie auf der Registerkarte **Anwendungseinstellungen** im linken Bereich die gewünschte Kategorie aus und ändern Sie im Ergebnisbereich auf der rechten Seite die Einstellungen der Richtlinie. Sie können die Einstellungen der Richtlinie in jeder Kategorie (jedem Abschnitt) ändern.

   Der Satz der Einstellungen ist davon abhängig, für welche Anwendung Sie eine Richtlinie erstellen. Weitere Informationen finden Sie hier:

   - Administrationsserver-Konfiguration
   - Richtlinieneinstellungen des Administrationsagenten
   - Hilfe zu Kaspersky Endpoint Security für Linux
   - Hilfe zu Kaspersky Endpoint Security für Windows

   Ausführliche Informationen über die Einstellungen anderer Sicherheitsanwendungen finden Sie in der Dokumentation der entsprechenden Anwendung.

   Beim Ändern der Einstellungen können Sie auf **Abbrechen** klicken, um den letzten Vorgang rückgängig zu machen.

9. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

   Es wird eine Benachrichtigung mit folgendem Inhalt angezeigt: **Die Richtlinie wird gespeichert und über die Hierarchie der Administrationsserver verteilt**.

   Wenn die Richtlinie die Validierung besteht, wird die folgende Benachrichtigung angezeigt: **Richtlinie wurde gespeichert**.

   Wenn die Richtlinie die Validierung nicht besteht, wird die folgende Benachrichtigung angezeigt: **Das Speichern und Verteilen der Richtlinie über die Hierarchie der Administrationsserver ist fehlgeschlagen. Wenden Sie sich an den Technischen Support**. Sie können die Richtlinieneinstellungen überprüfen, anpassen und es anschließend erneut versuchen. Wenn das Problem weiterhin besteht, wenden Sie sich an den Technischen Support.

Die Richtlinie wird in der Richtlinienliste angezeigt. Sobald die Richtlinie erstellt wurde, werden Ereignisse zu Richtlinienänderungen in ein SIEM-System exportiert, wenn diese Option aktiviert ist.

Allgemeine Richtlinieneinstellungen

Allgemein

Auf der Registerkarte **Allgemein** können Sie den Richtlinienstatus ändern und die Vererbung der Richtlinieneinstellungen anpassen:

- Im Block **Richtlinienstatus** können Sie einen der Richtlinienmodi auswählen:
  - **Aktiv**

    Bei Auswahl dieser Option wird die Richtlinie aktiv.

    Diese Variante ist standardmäßig ausgewählt.

- **Mobil**

  Bei Auswahl dieser Option wird die Richtlinie aktiv, sobald das Gerät vom Unternehmensnetzwerk getrennt wird.

- **Inaktiv**

  Bei Auswahl dieser Option wird die Richtlinie inaktiv, aber im Ordner **Richtlinien** gespeichert. Bei Bedarf kann die Richtlinie aktiviert werden.

- In der Einstellungsgruppe **Vererbung von Einstellungen** können Sie Einstellungen für die Vererbung der Richtlinie anpassen:

  - **Einstellungen aus übergeordneter Richtlinie erben**

    Ist diese Option aktiviert, so werden die Werte der Richtlinieneinstellungen aus der Richtlinie der obersten Hierarchie-Ebene vererbt und können nicht geändert werden.

    Diese Option ist standardmäßig aktiviert.

  - **Vererbung der Einstellungen an untergeordnete Richtlinien erzwingen**

    Ist diese Option aktiviert, so werden die folgenden Aktionen ausgeführt, nachdem die Richtlinienänderungen übernommen wurden:

    - Einstellungen der Richtlinie werden in die Tochter-Richtlinien, d.h. in die Richtlinien der untergeordneten Administrationsgruppen, übertragen.

    - Im Block **Einstellungen erben** des Abschnitts **Allgemein** im Eigenschaftenfenster aller untergeordneten Richtlinien wird die Option **Einstellungen aus Richtlinie der höheren Ebene erben** automatisch aktiviert.

    Ist diese Option aktiviert, so können die Einstellungen der untergeordneten Richtlinien nicht geändert werden.

    Diese Option ist standardmäßig deaktiviert.

Konfiguration von Ereignissen

Auf der Registerkarte **Konfiguration von Ereignissen** können Sie die Ereignisprotokollierung und die Benachrichtigung über Ereignisse konfigurieren. Die Ereignisse werden anhand der Ereigniskategorie auf folgende Registerkarten aufgeteilt:

- **Kritisch**

  Der Abschnitt **Kritisch** wird in den Eigenschaften der Richtlinie des Administrationsagenten nicht angezeigt.

- **Funktionsfehler**

- **Warnung**

- **Information**

Jeder Abschnitt enthält eine Liste mit Ereignistypen und der Standard-Speicherdauer des Ereignisses auf dem Administrationsserver (in Tagen). Mit einem Klick auf einen Ereignistyp können Sie die folgenden Einstellungen festlegen:

- **Ereignisregistrierung**

Sie können angeben, wie viele Tage und an welchem Ort das Ereignis gespeichert werden soll:

- **Mittels Syslog in ein SIEM-System exportieren**
- **Im System-Ereignisprotokoll des Geräts speichern**
- **Im System-Ereignisprotokoll des Administrationsservers speichern**

- **Ereignisbenachrichtigungen**

  Sie können bestimmen, ob Sie auf eine der folgenden Arten über das Ereignis benachrichtigt werden möchten:

  - **Per E-Mail benachrichtigen**
  - **Per SMS benachrichtigen**
  - **Durch den Start einer ausführbaren Datei oder eines Skriptes benachrichtigen**
  - **Per SNMP benachrichtigen**

  Standardmäßig werden die Benachrichtigungseinstellungen verwendet, die auf der Registerkarte "Eigenschaften des Administrationsservers" angegeben sind (z. B. Empfängeradresse). Wenn Sie möchten, können Sie diese Einstellungen auf den Registerkarten **E-Mail**, **SMS** und **Start einer ausführbaren Datei** ändern.

Die Registerkarte **Konfiguration von Ereignissen** zeigt Benachrichtigungen an, wenn neue Ereignistypen hinzugefügt wurden (z. B. in einer neuen Version der Anwendung) und erlaubt Ihnen das Anwenden der neuen Einstellungen durch das Anklicken der Schaltfläche **Speichern** oder **Speichern und schließen**.

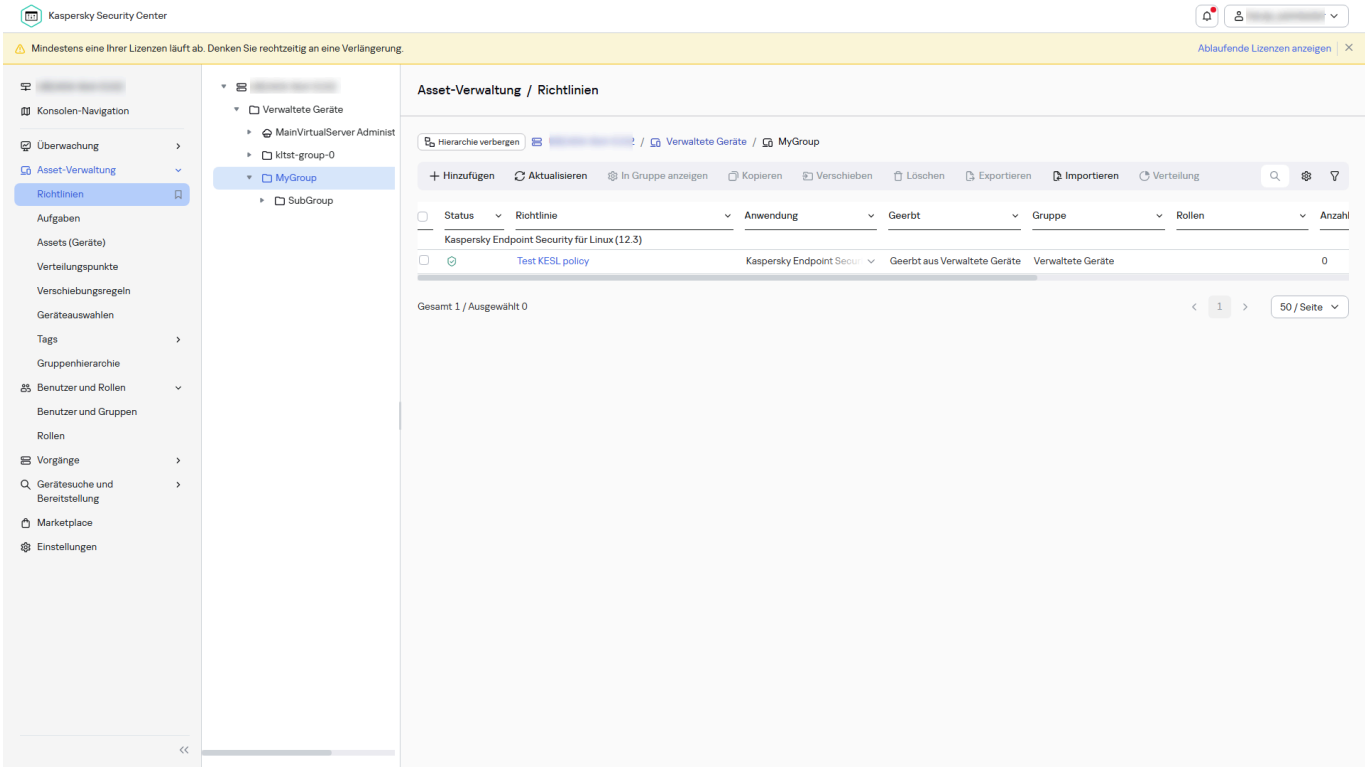
Revisionsverlauf

Auf der Registerkarte **Revisionsverlauf** können Sie eine Liste mit Revisionen der Richtlinie anzeigen, Richtlinienrevisionen vergleichen und bei Bedarf ein Rollback der Änderungen an der Richtlinie vornehmen.

Richtlinie ändern

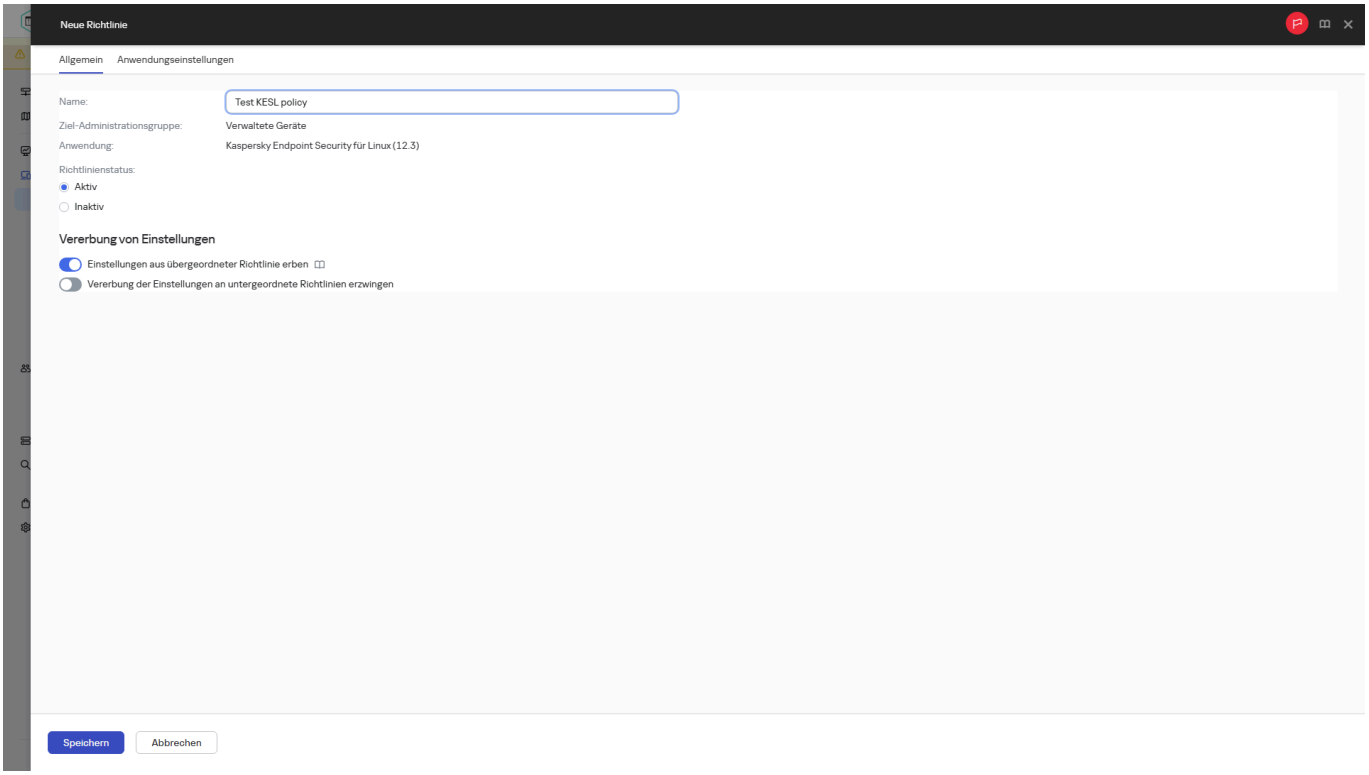
Um eine Richtlinie zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.



2. Klicken Sie auf die Richtlinie, die Sie ändern möchten.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.



3. Geben Sie die Allgemeinen Einstellungen und Einstellungen der Anwendung an, für welches Sie eine Richtlinie erstellen. Weitere Informationen finden Sie hier:

   - Administrationsserver-Konfiguration
   - Richtlinieneinstellungen des Administrationsagenten
   - Hilfe zu Kaspersky Endpoint Security für Linux
   - Hilfe zu Kaspersky Endpoint Security für Windows

   Ausführliche Informationen über die Einstellungen anderer Sicherheitsanwendungen finden Sie in der Dokumentation zu dieser Anwendung.

4. Klicken Sie auf die Schaltfläche **Speichern**.

   Es wird eine Benachrichtigung mit folgendem Inhalt angezeigt: **Die Richtlinie wird gespeichert und über die Hierarchie der Administrationsserver verteilt**.

   Wenn die Richtlinie die Validierung besteht, wird die folgende Benachrichtigung angezeigt: **Richtlinie wurde gespeichert**.

   Wenn die Richtlinie die Validierung nicht besteht, wird die folgende Benachrichtigung angezeigt: **Das Speichern und Verteilen der Richtlinie über die Hierarchie der Administrationsserver ist fehlgeschlagen. Wenden Sie sich an den Technischen Support**. Sie können die Richtlinieneinstellungen überprüfen, anpassen und es anschließend erneut versuchen. Wenn das Problem weiterhin besteht, wenden Sie sich an den Technischen Support.

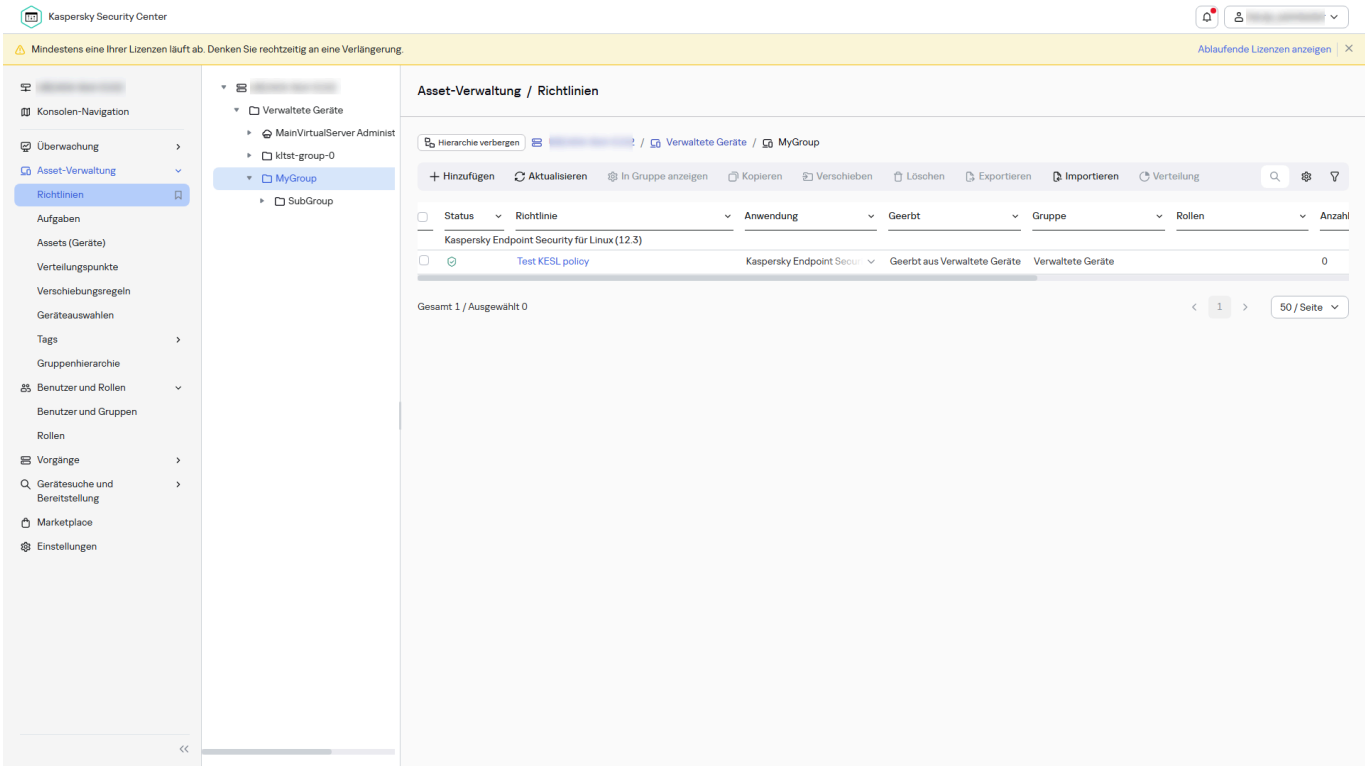
Die Änderungen der Richtlinie werden in den Eigenschaften der Richtlinie gespeichert und im Abschnitt **Revisionsverlauf** angezeigt. Sobald die Richtlinie geändert wurde, werden Ereignisse zu Richtlinienänderungen in ein SIEM-System exportiert, wenn diese Option aktiviert ist.

Bei Bedarf können Sie Richtlinienrevisionen vergleichen. Diese Option ist für die Richtlinien der folgenden Komponenten verfügbar: Administrationsserver, Administrationsagent, Kaspersky Endpoint Security für Windows (beginnend ab Version 14.0 des Web-Plug-ins) und Kaspersky Endpoint Security for Mac (beginnend ab Version 12.2.1 Patch A des Web-Plug-ins).

Option zur Vererbung einer Richtlinie aktivieren und deaktivieren

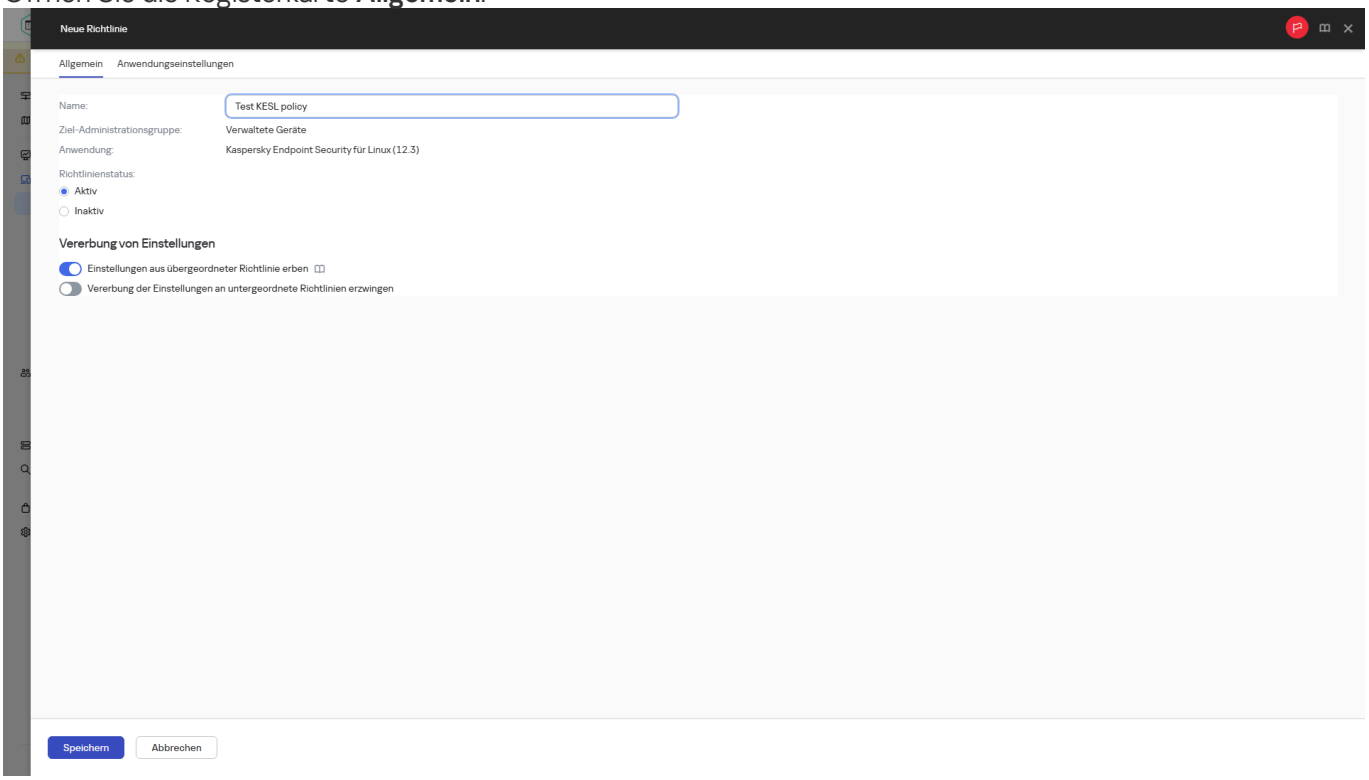
So aktivieren oder deaktivieren Sie die Vererbungsoption in einer Richtlinie:

1. Öffnen Sie die erforderliche Richtlinie.



Die Liste der Richtlinien

2. Öffnen Sie die Registerkarte **Allgemein**.



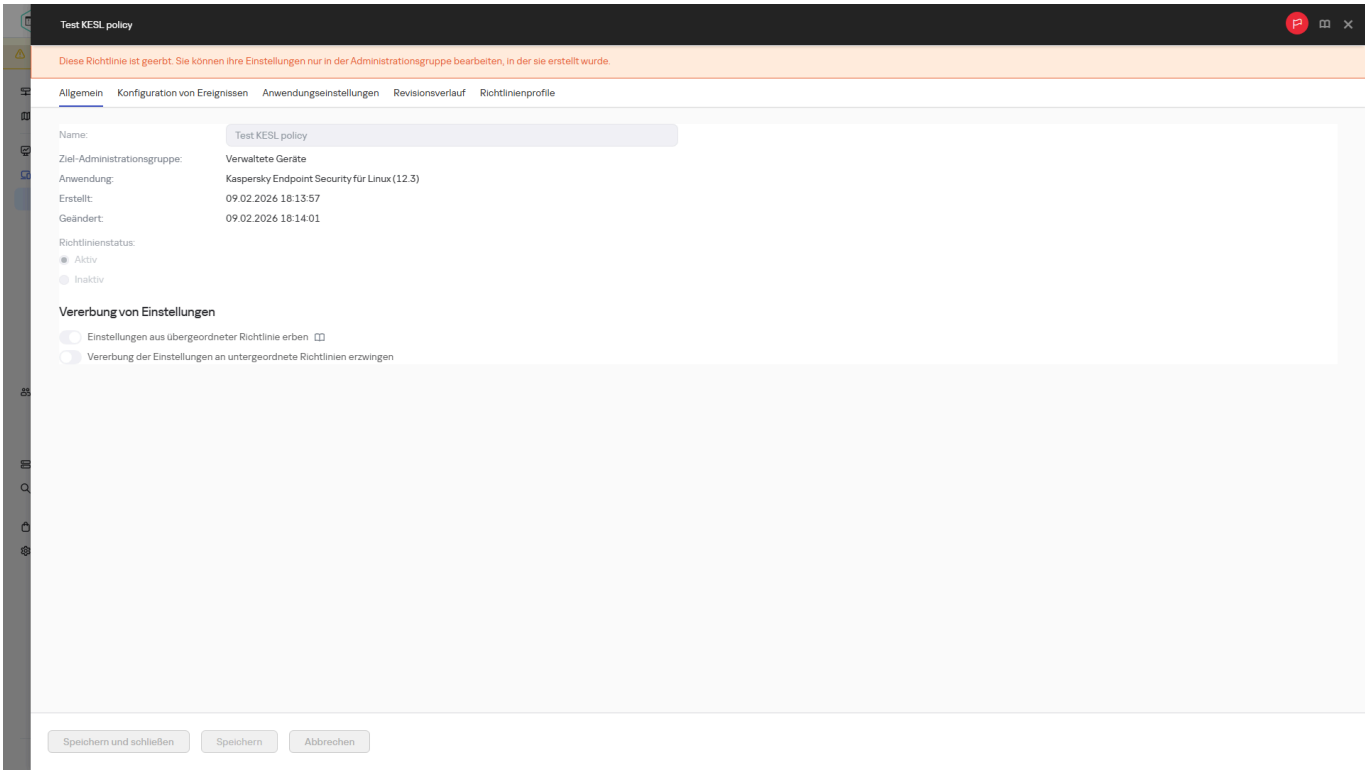
Eine neue Richtlinie erstellen

3. Aktivieren oder Deaktivieren der Richtlinienvererbung:

   - Wenn Sie **Einstellungen aus übergeordneter Richtlinie erben** in einer untergeordneten Richtlinie aktivieren und ein Administrator einige Einstellungen in der übergeordneten Richtlinie sperrt, können Sie diese Einstellungen in der untergeordneten Richtlinie nicht ändern.

   - Wenn Sie die Option **Einstellungen aus übergeordneter Richtlinie erben** für eine untergeordnete Gruppe deaktivieren, können Sie alle Einstellungen in der untergeordneten Gruppe bearbeiten, selbst wenn einige Einstellungen in der übergeordneten Richtlinie mit einem Schloss gesperrt sind.

   - Wenn Sie **Vererbung der Einstellungen an untergeordnete Richtlinien erzwingen** in der übergeordneten Gruppe aktivieren, wird dadurch **Einstellungen aus übergeordneter Richtlinie erben** für alle untergeordneten Richtlinien aktiviert. In diesem Fall kann diese Option nicht für untergeordnete Richtlinien deaktiviert werden. Alle Einstellungen, die in der übergeordneten Richtlinie gesperrt sind, werden zwangsweise an untergeordnete Gruppen vererbt und können in den untergeordneten Gruppen nicht bearbeitet werden.



Gesperrte Richtlinieneinstellungen

4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern, oder klicken Sie auf die Schaltfläche **Abbrechen**, um sie zu verwerfen.

Standardmäßig ist die Option **Einstellungen aus übergeordneter Richtlinie erben** für eine neue Richtlinie aktiviert.

Wenn eine Richtlinie über Profile verfügt, erben alle untergeordneten Richtlinien diese Profile.

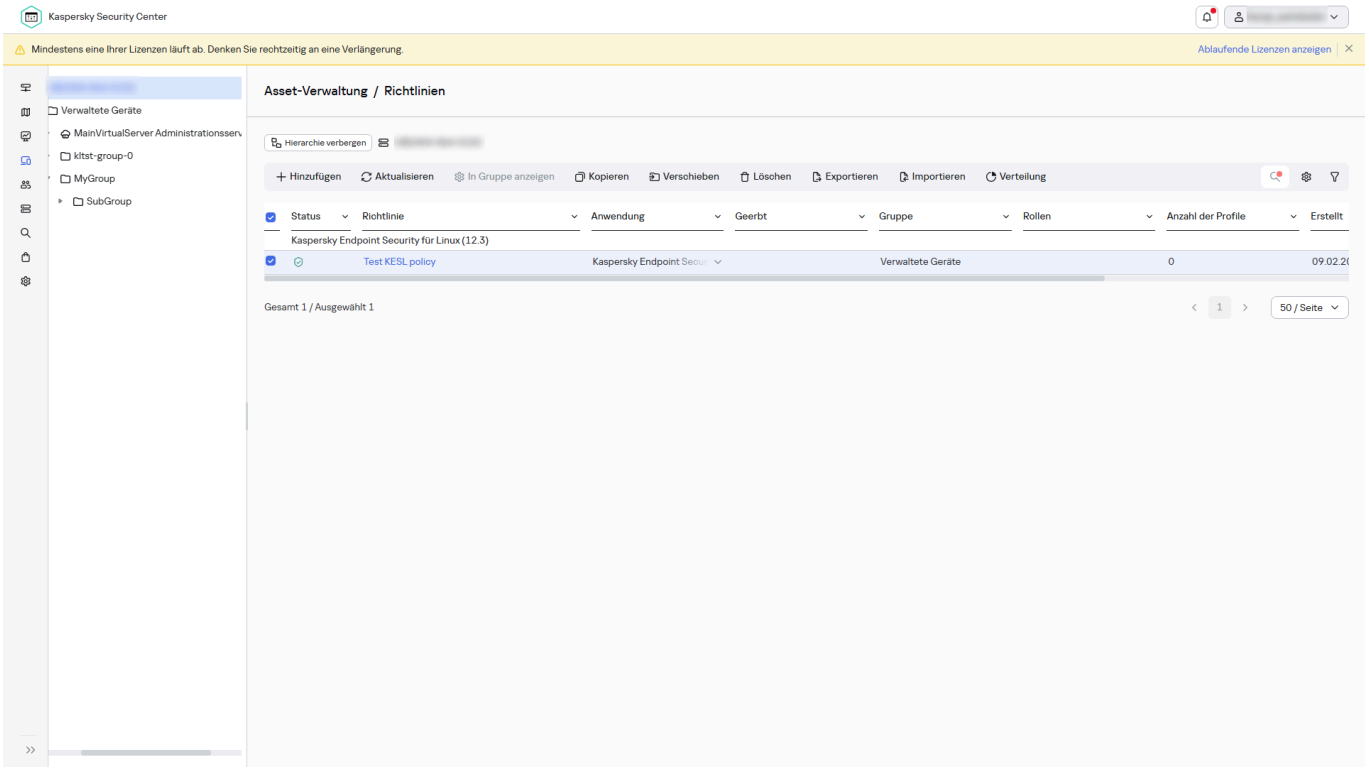
Richtlinien kopieren

Richtlinien können von einer Administrationsgruppe zu einer anderen kopiert werden.

Um eine Richtlinie zu einer anderen Administrationsgruppe zu kopieren, gehen Sie wie folgt vor:

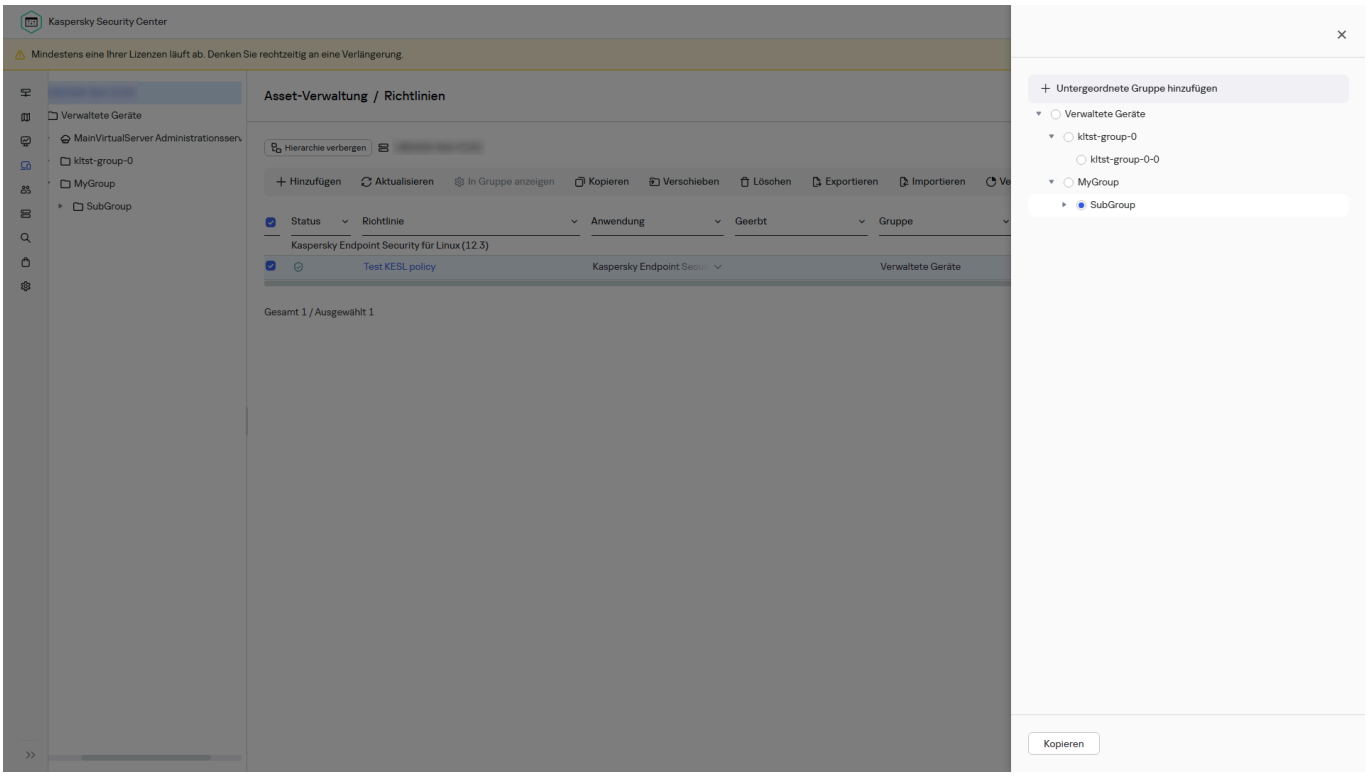
1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

2. Aktivieren Sie die Kontrollkästchen neben der Richtlinie (oder den Richtlinien), die Sie kopieren möchten.



3. Klicken Sie auf die Schaltfläche **Kopieren**.

   Im rechten Bereich des Bildschirms erscheint die Strukturansicht der Administrationsgruppen.



4. Wählen Sie in der Strukturansicht die Zielgruppe aus. Das ist die Gruppe, zu der Sie die Richtlinie (oder die Richtlinien) kopieren möchten.

5. Klicken Sie auf die Schaltfläche **Kopieren** am unteren Rand des Bildschirms.

6. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Die Richtlinie bzw. Richtlinien werden samt allen Profilen zur Zielgruppe kopiert. Der Status jeder kopierten Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit auf **Aktiv** setzen.

Wenn die gewählte Richtlinienliste bereits eine Richtlinie mit dem gleichen Namen wie die zu verschiebende Richtlinie enthält, wird dem Namen der verschobenen Richtlinie eine Endung der Form (<laufende Nummer>) angehängt. Beispiel: (1).

Richtlinie verschieben

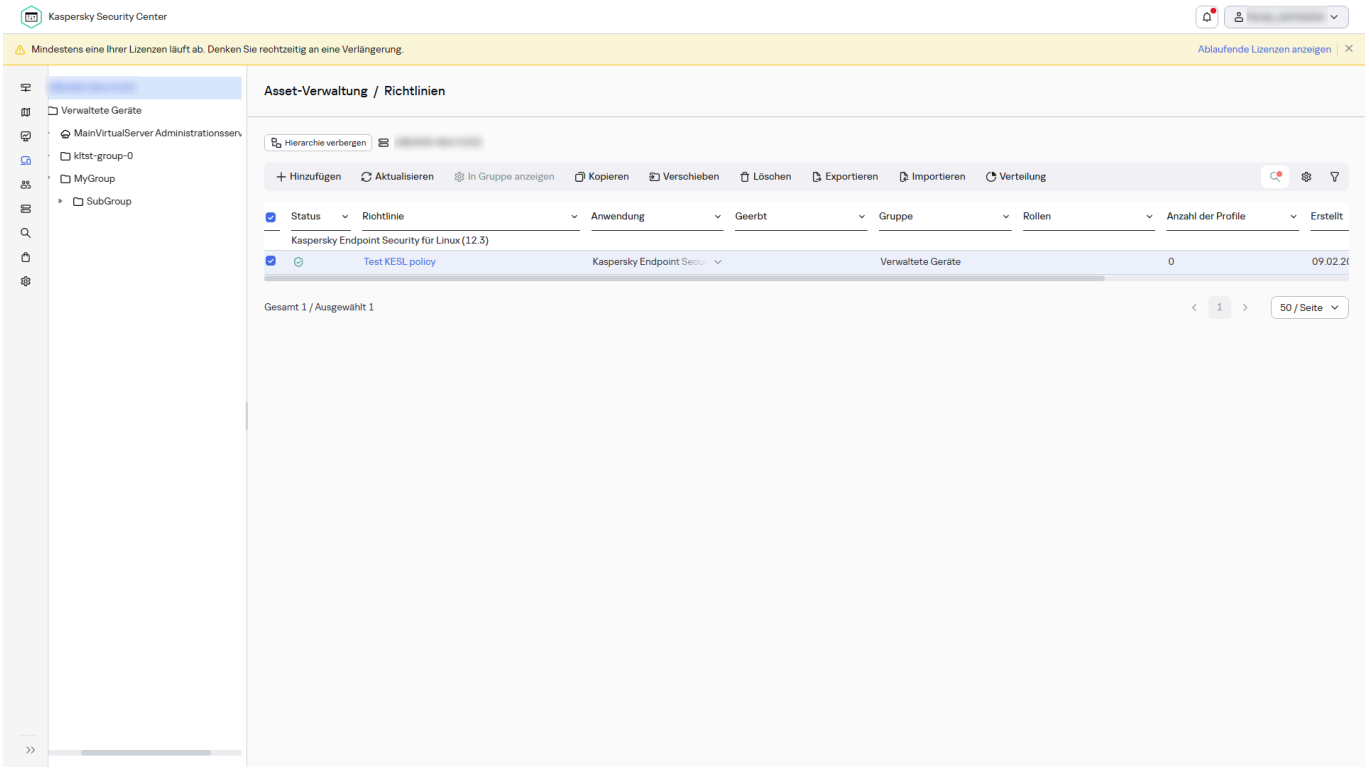
Richtlinien können von einer Administrationsgruppe zu einer anderen verschoben werden. Angenommen, Sie möchten eine Gruppe löschen, aber ihre Richtlinien für eine andere Gruppe verwenden. In diesem Fall können Sie die Richtlinie der alten Gruppe zur neuen Gruppe verschieben, bevor Sie die Gruppe löschen.

Beim Verschieben einer Richtlinie in eine andere Verwaltungsgruppe wird der Revisionsverlauf der Richtlinie gelöscht. Auf der Registerkarte **Revisionsverlauf** werden nur Informationen zur letzten Änderung angezeigt.

Um eine Richtlinie zu einer anderen Administrationsgruppe zu verschieben, gehen Sie wie folgt vor:

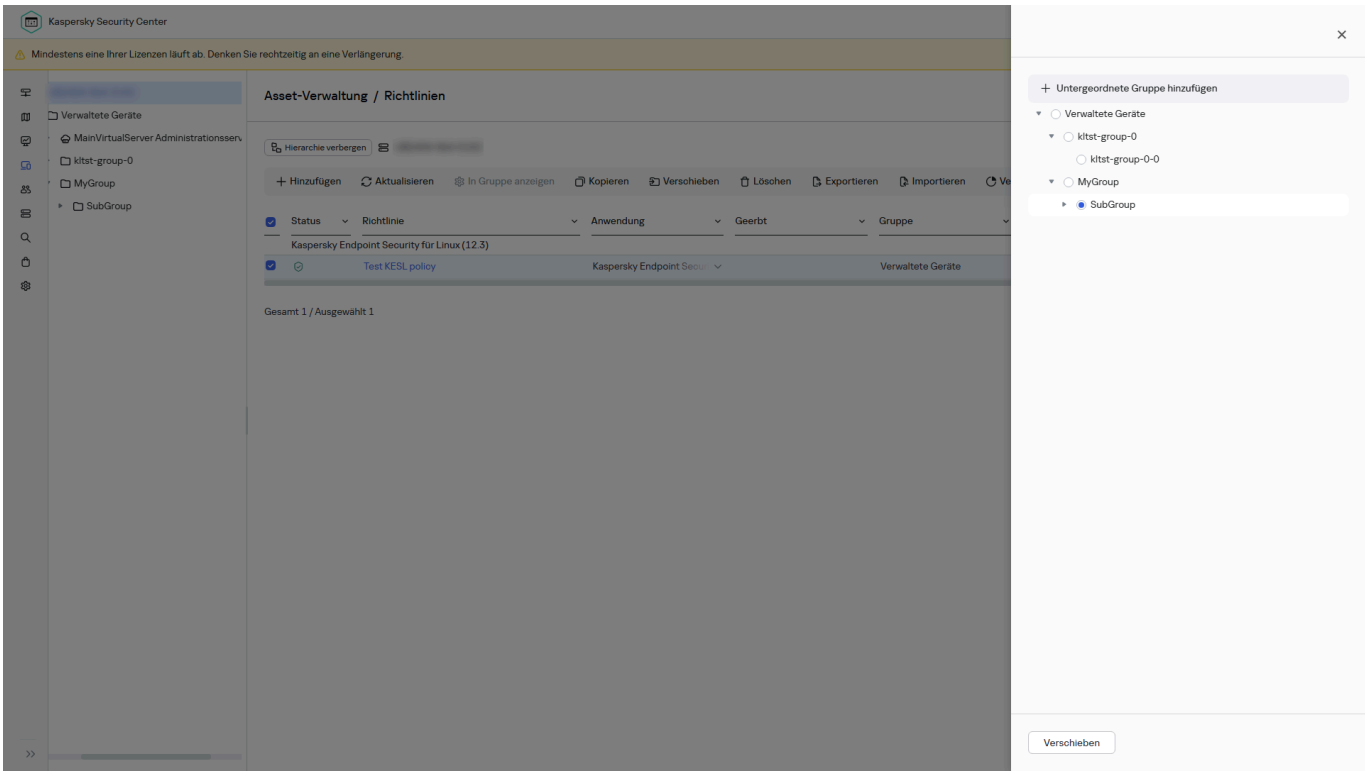
1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

2. Aktivieren Sie die Kontrollkästchen neben der Richtlinie (oder den Richtlinien), die Sie verschieben möchten.



3. Klicken Sie auf die Schaltfläche **Verschieben**.

   Im rechten Bereich des Bildschirms erscheint die Strukturansicht der Administrationsgruppen.



4. Wählen Sie in der Strukturansicht die Zielgruppe aus. Das ist die Gruppe, zu der Sie die Richtlinie (oder die Richtlinien) verschieben möchten.

5. Klicken Sie auf die Schaltfläche **Verschieben** am unteren Rand des Bildschirms.

6. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

   Wenn die Richtlinie nicht von der Quellgruppe geerbt wurde, wird sie samt allen Profilen zur Zielgruppe verschoben. Der Status der Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit auf **Aktiv** setzen.

   Wenn die Richtlinie von der Quellgruppe geerbt wurde, bleibt sie in der Quellgruppe erhalten. Sie wird samt allen Profilen zur Zielgruppe kopiert. Der Status der Richtlinie in der Zielgruppe ist **Inaktiv**. Sie können den Status jederzeit auf **Aktiv** setzen.

Wenn die gewählte Richtlinienliste bereits eine Richtlinie mit dem gleichen Namen wie die zu verschiebende Richtlinie enthält, wird dem Namen der verschobenen Richtlinie eine Endung der Form (<laufende Nummer>) angehängt. Beispiel: (1).

Richtlinien exportieren

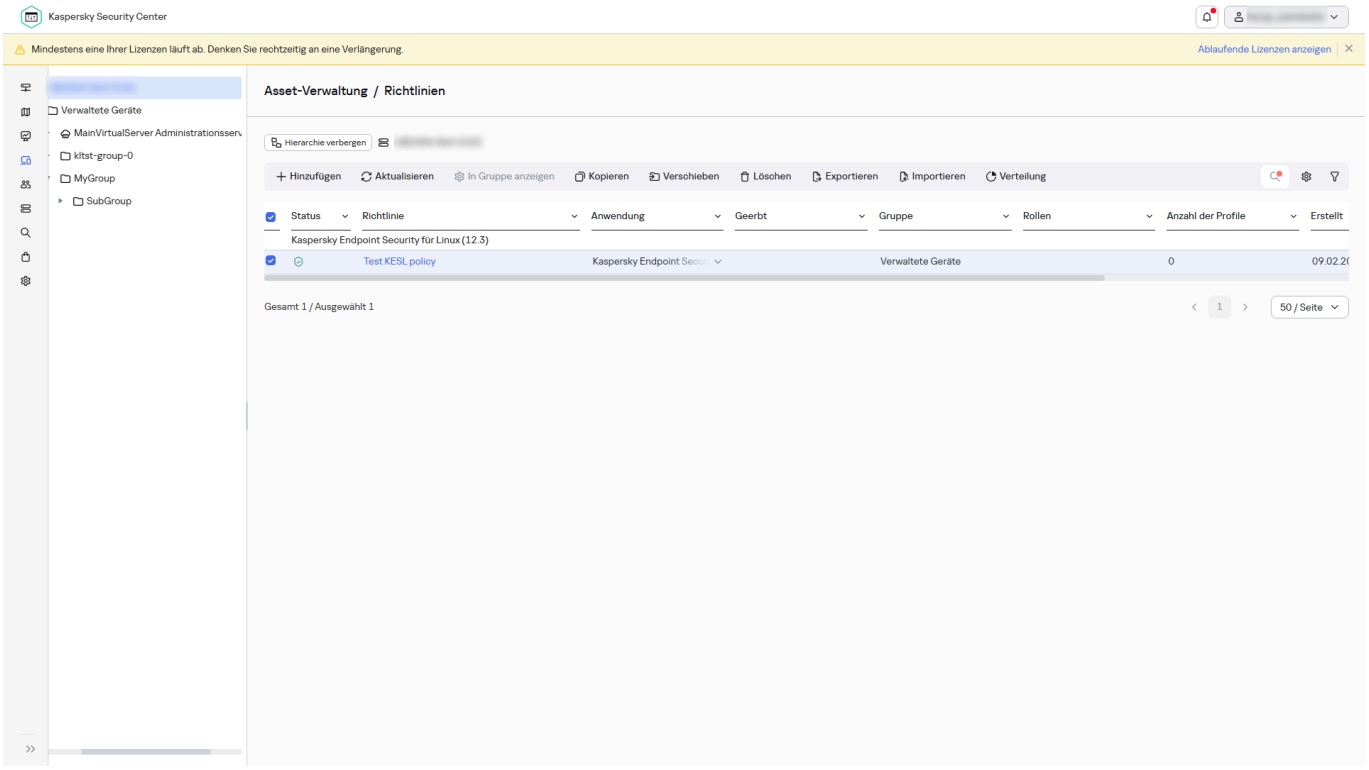
Mit Kaspersky Security Center Linux können Sie eine Richtlinie, deren Einstellungen und Richtlinienprofile in einer klp-Datei speichern. Sie können diese klp-Datei verwenden, um sowohl in Kaspersky Security Center Windows als auch in Kaspersky Security Center Linux die gespeicherte Richtlinie zu importieren.

Um eine Richtlinie zu exportieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

2. Aktivieren Sie das Kontrollkästchen neben der Richtlinie, die Sie installieren möchten.

Sie können nicht mehrere Richtlinien gleichzeitig exportieren. Wenn Sie mehr als eine Richtlinie auswählen, wird die Schaltfläche **Exportieren** deaktiviert.



Eine Richtlinie für den Export auswählen

3. Klicken Sie auf die Schaltfläche **Exportieren**.

4. Geben Sie im folgenden Fenster **Speichern unter** den Namen und den Pfad der Richtliniendatei an. Klicken Sie auf **Speichern**.

   Das Fenster **Speichern unter** wird nur angezeigt, wenn Sie Google Chrome, Microsoft Edge oder Opera verwenden. Wenn Sie einen anderen Browser verwenden, wird die Richtliniendatei automatisch im Ordner **Downloads** gespeichert.

Richtlinien importieren

Mit Kaspersky Security Center Linux können Sie eine Richtlinie aus einer klp-Datei importieren. Die klp-Datei enthält die exportierte Richtlinie, deren Einstellungen und Richtlinienprofile.

So importieren Sie eine Richtlinie:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

2. Klicken Sie auf die Schaltfläche **Importieren**.

3. Klicken Sie auf die Schaltfläche **Durchsuchen**, um eine Richtliniendatei auszuwählen, die Sie importieren möchten.

4. Geben Sie im folgenden Fenster den Pfad zur klp-Richtliniendatei an und klicken Sie anschließend auf die Schaltfläche **Öffnen**. Beachten Sie, dass Sie nur eine Richtliniendatei auswählen können.

   Die Verarbeitung der Richtlinien beginnt.

5. Nachdem die Richtlinie erfolgreich verarbeitet wurde, wählen Sie die Administrationsgruppe aus, auf die Sie die Richtlinie anwenden möchten.

6. Klicken Sie auf die Schaltfläche **Abgeschlossen**, um den Import der Richtlinie abzuschließen.

Die Benachrichtigung mit dem Resultat des Imports wird angezeigt. Wenn die Richtlinie erfolgreich importiert wurde, können Sie zum Anzeigen der Eigenschaften der Richtlinie auf den Link **Details** klicken.

Nach einem erfolgreichen Import wird die Richtlinie in der Liste der Richtlinien angezeigt. Die Einstellungen und Profile der Richtlinie werden ebenfalls importiert. Unabhängig vom Richtlinienstatus, der während des Exports ausgewählt wurde, ist die importierte Richtlinie inaktiv. Sie können den Richtlinienstatus in den Eigenschaften der Richtlinie ändern.

Wenn die neu importierte Richtlinie denselben Namen wie eine bereits vorhandene Richtlinie besitzt, wird der Name der importierten Richtlinie um den Index **(<nächste Sequenznummer>)** erweitert, zum Beispiel: **(1)**, **(2)**.

Erzwungene Synchronisierung

Obwohl Kaspersky Security Center Linux den Status, die Einstellungen, die Aufgaben und die Richtlinien für die verwalteten Geräte automatisch synchronisiert, kann es in bestimmten Situationen vorkommen, dass der Administrator genau wissen muss, ob die Synchronisierung für ein bestimmtes Gerät bereits ausgeführt wurde.

Synchronisation eines einzelnen Geräts

So erzwingen Sie die Synchronisierung zwischen dem Administrationsserver und dem verwalteten Gerät:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.

2. Klicken Sie auf den Namen des Geräts, das mit dem Administrationsserver synchronisiert werden soll.

   Ein Eigenschaftenfenster wird geöffnet, in dem der Abschnitt **Allgemein** ausgewählt ist.

3. Klicken Sie auf die Schaltfläche **Synchronisierung erzwingen**.

Die Anwendung synchronisiert das ausgewählte Gerät mit dem Administrationsserver.

Synchronisation mehrerer Geräte

So erzwingen Sie die Synchronisierung zwischen dem Administrationsserver und mehreren verwalteten Geräten:

1. Öffnen Sie die Geräteliste einer Administrationsgruppe oder einer Geräteauswahl:
   - Führen Sie eine Geräteauswahl durch, um die Geräteliste anzuzeigen.
   - Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)** und wählen Sie anschließend die Administrationsgruppe aus, welche die zu synchronisierenden Geräte enthält:
     - Für die Stammgruppe können Sie mit dem nächsten Schritt fortfahren.
     - Klicken Sie für eine Untergruppe im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen** und anschließend im neuen Fenster auf den Namen der Untergruppe.

       Der Pfad zur ausgewählten Gruppe wird im oben Bereich der Seite angezeigt. Bei Bedarf können Sie auf einen Link mit dem Namen der Administrationsgruppe klicken, um zu dieser Gruppe zu gelangen. Der letzte Link im Pfad ist standardmäßig inaktiv. Außerdem können Sie das Hierarchiefenster schließen, indem Sie auf die Schaltfläche **Hierarchie verbergen** klicken.
2. Aktivieren Sie die Kontrollkästchen neben den Geräten, die Sie mit dem Administrationsserver synchronisieren möchten.
3. Klicken Sie über der Liste der verwalteten Geräte auf die Schaltfläche mit den 3 Punkten (...) und klicken Sie anschließend auf die Schaltfläche **Synchronisierung erzwingen**.

   Die Anwendung synchronisiert die ausgewählten Geräte mit dem Administrationsserver.
4. Prüfen Sie in der Geräteliste, dass sich die Zeit der letzten Verbindung zum Administrationsserver für die ausgewählten Geräte auf die aktuelle Zeit geändert hat. Wenn sich die Uhrzeit nicht geändert hat, aktualisieren Sie den Seiteninhalt, indem Sie auf die Schaltfläche **Aktualisieren** klicken.

Die ausgewählten Geräte wurden mit dem Administrationsserver synchronisiert.

Anzeigen des Übermittlungszeitpunktes einer Richtlinie

Nach dem Ändern einer Richtlinie für eine Kaspersky-Anwendung auf dem Administrationsserver kann der Administrator auch prüfen, ob die geänderte Richtlinie an ein bestimmtes verwaltetes Gerät übermittelt wurde. Eine Richtlinie kann während einer regulären oder einer erzwungenen Synchronisierung übermittelt werden.

Um den Zeitpunkt (Datum und Uhrzeit) anzuzeigen, zu dem eine Anwendungsrichtlinie an ein verwaltetes Gerät übermittelt wurde:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.
2. Klicken Sie auf den Namen des Geräts, das mit dem Administrationsserver synchronisiert werden soll.

   Ein Eigenschaftenfenster wird geöffnet, in dem der Abschnitt **Allgemein** ausgewählt ist.
3. Klicken Sie auf die Registerkarte **Anwendungen**.
4. Wählen Sie die Anwendung aus, für das Sie das Datum der Richtliniensynchronisierung anzeigen möchten.

   Das Fenster mit der Anwendungsrichtlinie wird geöffnet; dabei ist der Abschnitt **Allgemein** ausgewählt und das Datum und die Uhrzeit der Übertragung der Richtlinie werden angezeigt.

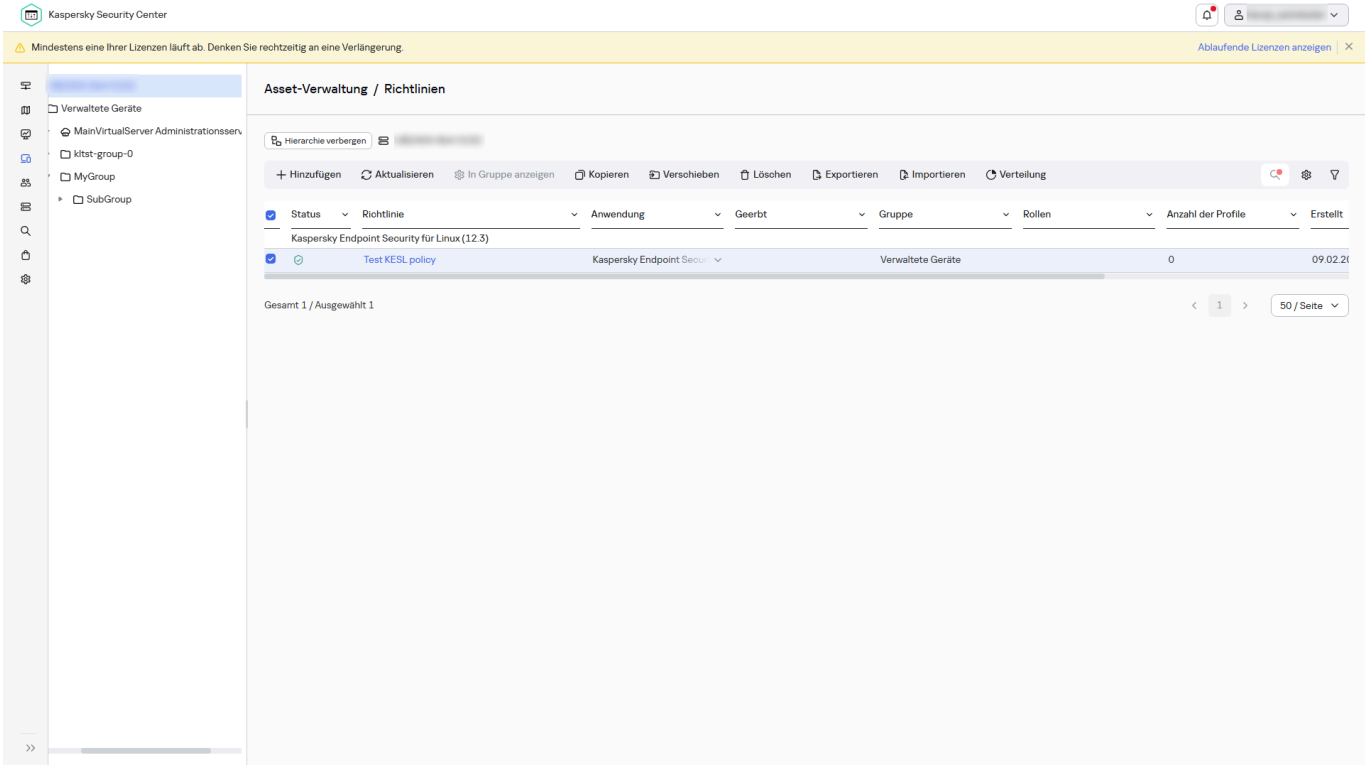
Diagramm zum Status der Richtlinienverteilung anzeigen

In Kaspersky Security Center Linux können Sie den Richtlinienstatus für jedes Gerät in einem Diagramm für den Status der Richtlinienverteilung anzeigen.

So zeigen Sie das Statusdiagramm für die Richtlinienverteilung für jedes Gerät an:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

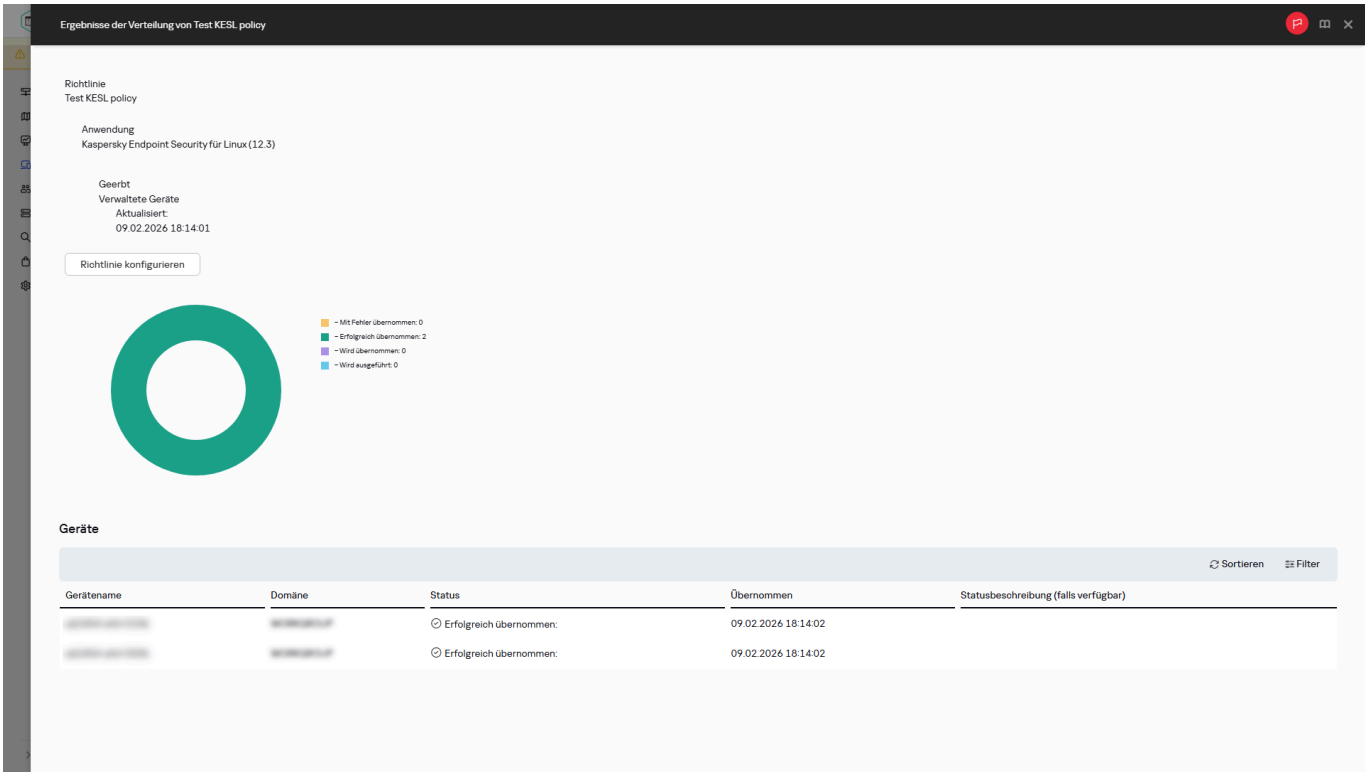
2. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, für die Sie den Verteilungsstatus auf Geräten anzeigen wollen.



Die Liste der Richtlinien

3. Wählen Sie im folgenden Menü den Link **Verteilung** aus.

Das Fenster **<Name der Richtlinie> Ergebnisse der Verteilung** wird geöffnet.



Die Ergebnisse der Verteilung der Richtlinie

4. Im folgenden Fenster **<Name der Richtlinie> Ergebnisse der Verteilung** wird eine **Statusbeschreibung** der Richtlinie angezeigt.

Sie können die Anzahl der angezeigten Ergebnisse in der Liste der Richtlinienverteilung ändern. Die maximale Anzahl an Geräten ist 100.000.

Um die Anzahl der in der Liste mit den Ergebnissen der Richtlinienverteilung angezeigten Geräte zu ändern, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Einstellungen der Benutzeroberfläche**.
2. Geben Sie für **Obergrenze der in den Ergebnissen der Richtlinienverteilung angezeigten Geräte** die Anzahl an Geräten ein (bis zu 100.000).

   Die standardmäßige Anzahl beträgt 5000.
3. Klicken Sie auf die Schaltfläche **Speichern**.

   Die Einstellungen werden gespeichert und übernommen.

Richtlinie nach dem Ereignis "Virenangriff" automatisch aktivieren

Damit beim Ereignis "Virenangriff" automatisch eine Richtlinie aktiviert wird:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster für die Einstellungen des Administrationsservers wird mit der Registerkarte **Allgemein** geöffnet.
2. Wählen Sie den Abschnitt **Virenangriff** aus.

3. Klicken Sie im rechten Bereich auf den Link **Richtlinien so konfigurieren, dass sie aktiviert werden, wenn ein Ereignis des Typs "Virenangriff" auftritt**.

   Das Fenster **Aktivierung von Richtlinien** wird geöffnet.

4. Wählen Sie im Abschnitt der Komponente, die den Virenangriff erkannt hat (Anti-Virus für Workstations und Dateiserver, Anti-Virus für E-Mail-Server oder Anti-Virus für Perimeterschutz) die Optionsschaltfläche neben dem gewünschten Eintrag und klicken Sie auf **Hinzufügen**.

   Ein Fenster mit der Administrationsgruppe **Verwaltete Geräte** wird geöffnet.

5. Klicken Sie auf den Chevron-Symbol (›) neben **Verwaltete Geräte**.

   Eine Hierarchie der Administrationsgruppen und der entsprechenden Richtlinien wird angezeigt.

6. Klicken Sie in der Hierarchie der Administrationsgruppen und Richtlinien auf den Namen einer oder mehrere Richtlinien, die aktiviert werden sollen, wenn ein Virenangriff erkannt wird.

   Um alle Richtlinien in der Liste oder in einer Gruppe auszuwählen, aktivieren Sie das Kontrollkästchen neben dem entsprechenden Namen.

7. Klicken Sie auf die Schaltfläche **Speichern**.

   Das Fenster mit der Hierarchie der Administrationsgruppen und Richtlinien wird geschlossen.

Die ausgewählten Richtlinien werden in die Liste der Richtlinien aufgenommen, die aktiviert werden, wenn ein Virenangriff erkannt wird. Bei einem Virenangriff werden die ausgewählten Richtlinien unabhängig davon aktiviert, ob sie aktiv oder inaktiv sind.

Wird eine Richtlinie aufgrund des Ereignisses "Virenangriff" aktiviert, ist eine Rückkehr zur vorherigen Richtlinie nur manuell möglich.

Richtlinien löschen

Eine nicht mehr benötigte Richtlinie kann gelöscht werden. Sie können nur Richtlinien löschen, die in der angegebenen Administrationsgruppe nicht geerbt sind. Eine geerbte Richtlinie kann nur in der Gruppe der höheren Ebene gelöscht werden, für die sie erstellt wurde.

Um eine Richtlinie zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

2. Aktivieren Sie die Kontrollkästchen neben der Richtlinie, die Sie löschen möchten, und klicken Sie auf **Löschen**.

   Die Schaltfläche **Löschen** ist nicht verfügbar (abgeblendet), wenn Sie eine geerbte Richtlinie auswählen.

3. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

Die Richtlinie wird samt allen Profilen gelöscht. Sobald die Richtlinie gelöscht wurde, werden Ereignisse zu Richtlinienänderungen in ein SIEM-System exportiert, wenn diese Option aktiviert ist.

Richtlinienprofile verwalten

Dieser Abschnitt beschreibt die Verwaltung von Richtlinienprofilen und enthält Informationen zum Anzeigen der Profile einer Richtlinie, zum Ändern der Priorität eines Richtlinienprofils, zum Erstellen eines Richtlinienprofils, zum Kopieren eines Richtlinienprofils, zum Erstellen einer Regel zur Aktivierung eines Richtlinienprofils und zum Löschen, Exportieren und Importieren eines Richtlinienprofils.

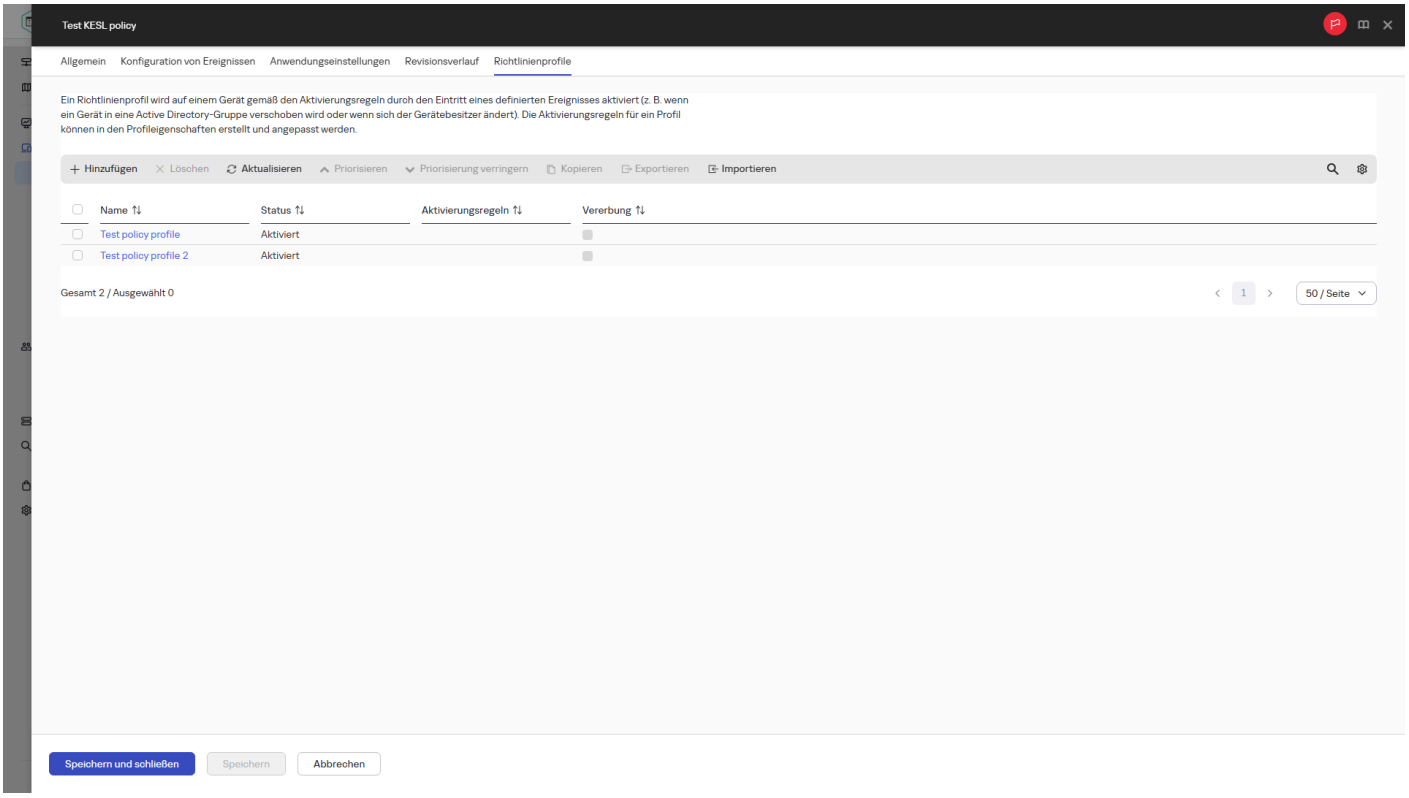
Profile einer Richtlinie anzeigen

So zeigen Sie Profile einer Richtlinie an:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.
2. Klicken Sie auf den Namen der Richtlinie, deren Profile Sie anzeigen möchten.

   Das Fenster mit den Eigenschaften der Richtlinie wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.
3. Öffnen Sie die Registerkarte **Richtlinienprofile**.

Daraufhin wird die Liste der Richtlinienprofile in Tabellenformat geöffnet. Wenn die Richtlinie über keine Profile verfügt, wird eine leere Tabelle angezeigt.



Die Liste der Richtlinienprofile

Priorität eines Richtlinienprofils ändern

Um die Priorität eines Richtlinienprofils zu ändern, gehen Sie wie folgt vor:

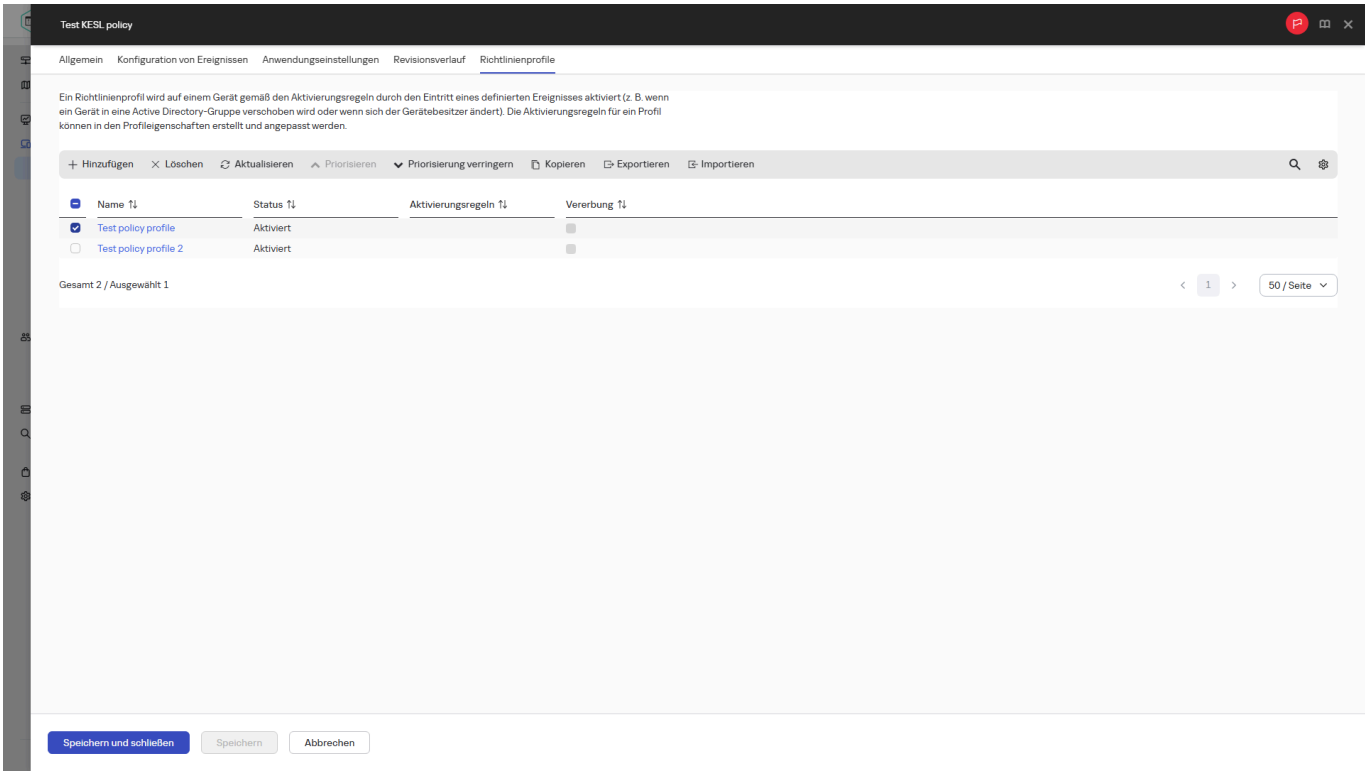
1. Gehen Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Aktivieren Sie auf der Registerkarte **Richtlinienprofile** das Kontrollkästchen neben dem Richtlinienprofil, dessen Priorität Sie ändern möchten.

3. Ändern Sie die Position des Richtlinienprofils in der Liste, indem Sie auf **Priorisieren** oder **Priorisierung verringern** klicken.

   Je höher ein Richtlinienprofil in der Liste steht, desto höher ist seine Priorität.



4. Klicken Sie auf die Schaltfläche **Speichern**.

Die Priorität des ausgewählten Richtlinienprofils wird verändert und angewendet.

Richtlinienprofil erstellen

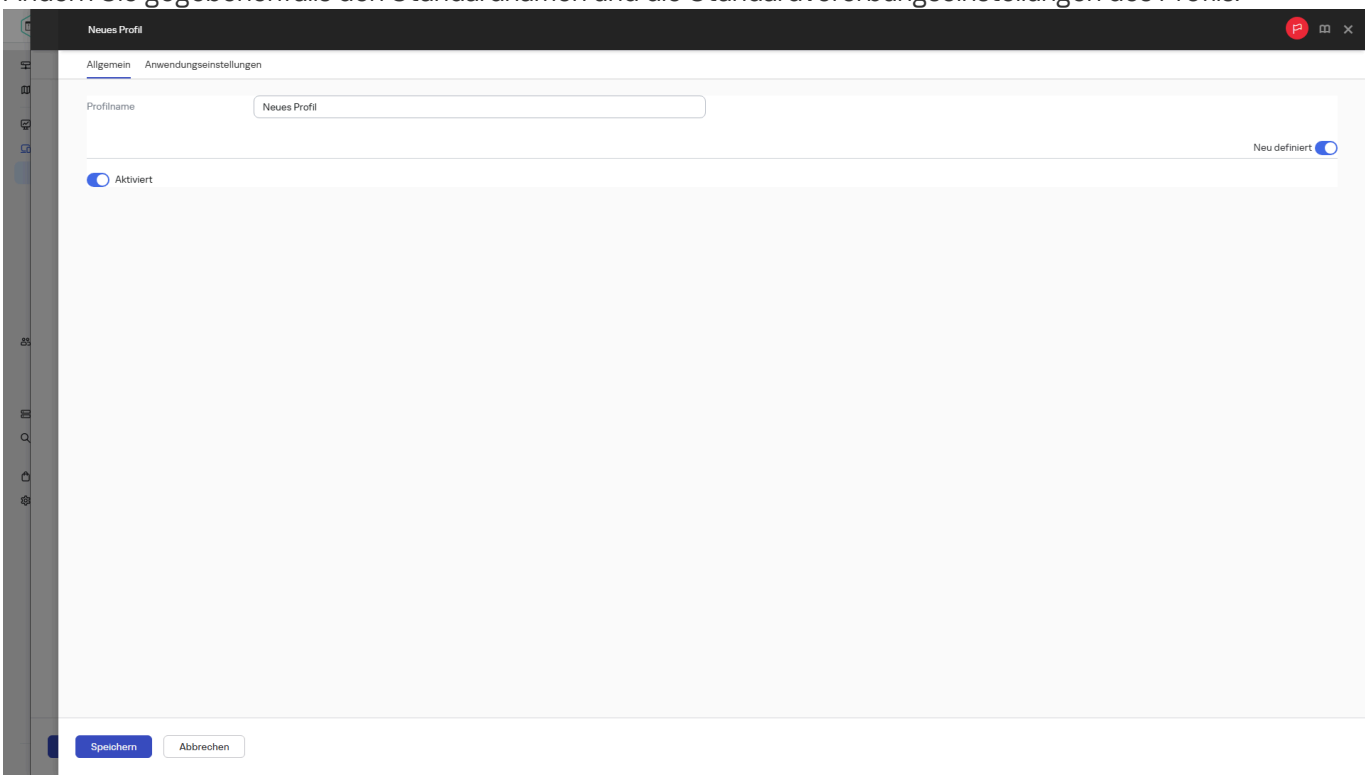
Um ein Richtlinienprofil zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet. Wenn die Richtlinie über keine Profile verfügt, wird eine leere Tabelle angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Ändern Sie gegebenenfalls den Standardnamen und die Standardvererbungseinstellungen des Profils.



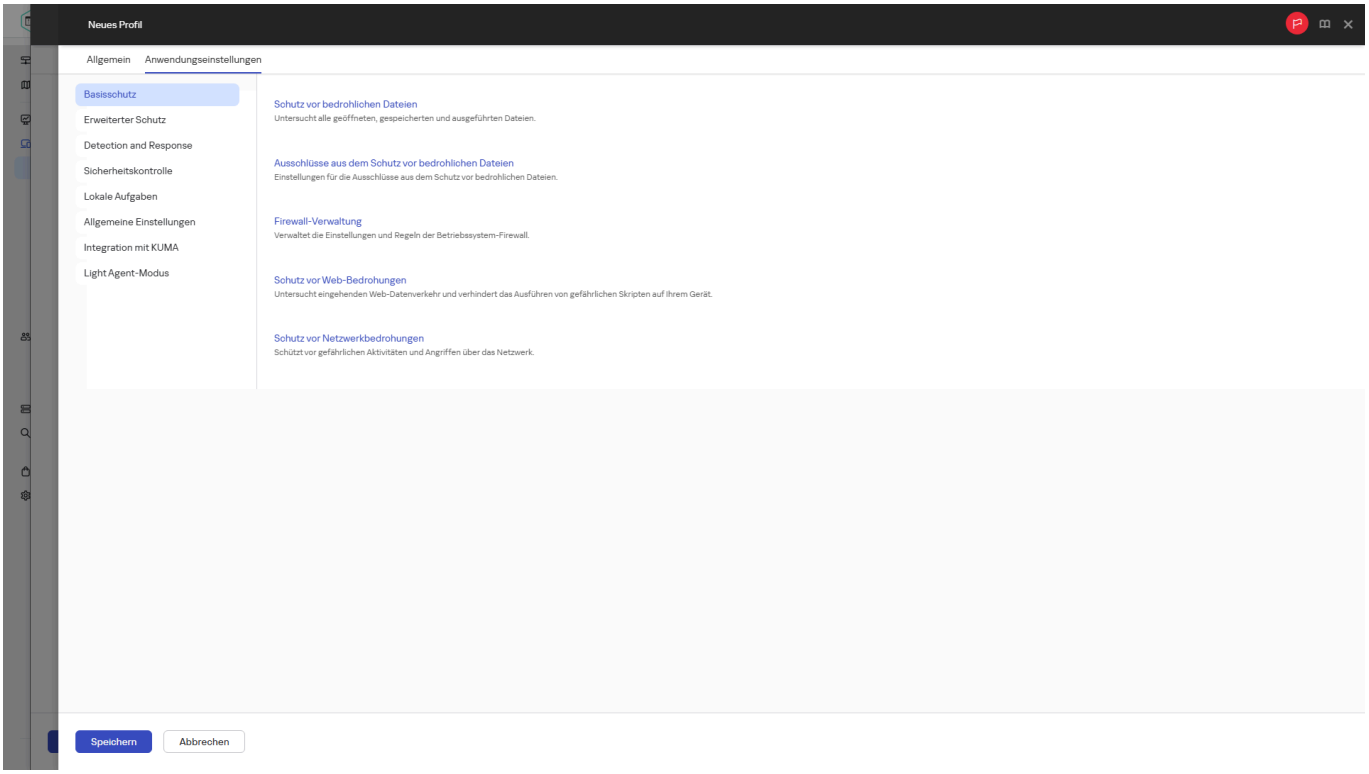
Erstellung eines neuen Richtlinienprofils

4. Wählen Sie die Registerkarte **Anwendungseinstellungen** aus.

   Alternativ dazu können Sie auf **Speichern** klicken und beenden. Das Profil, das Sie erstellt haben, wird in der Liste der Richtlinienprofile angezeigt, und Sie können seine Einstellungen später anpassen.

5. Wählen Sie auf der Registerkarte **Anwendungseinstellungen** im linken Bereich die gewünschte Kategorie aus und ändern Sie im Ergebnisbereich auf der rechten Seite die Einstellungen für das Profil. Sie können die Einstellungen des Richtlinienprofils in jeder Kategorie (jedem Abschnitt) ändern.

Beim Ändern der Einstellungen können Sie auf **Abbrechen** klicken, um den letzten Vorgang rückgängig zu machen.



Angeben der Einstellungen für das Richtlinienprofil

6. Klicken Sie auf **Speichern**, um das Profil zu speichern.

Das Profil wird in der Liste der Richtlinienprofile angezeigt.

Richtlinienprofil kopieren

Sie können ein Richtlinienprofil zur aktuellen oder zu einer anderen Richtlinie kopieren, wenn Sie z. B. identische Profile für verschiedene Richtlinien festlegen möchten. Das Kopieren von Profilen ist auch dann nützlich, wenn Sie zwei oder mehrere Profile anlegen möchten, deren Einstellungen sich nur minimal unterscheiden.

Um ein Richtlinienprofil zu kopieren, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet. Wenn die Richtlinie über keine Profile verfügt, wird eine leere Tabelle angezeigt.

2. Wählen Sie auf der Registerkarte **Richtlinienprofile** das Richtlinienprofil aus, das Sie kopieren möchten.

3. Klicken Sie auf die Schaltfläche **Kopieren**.

4. Wählen Sie im nächsten Fenster die Richtlinie aus, zu der Sie das Profil kopieren möchten.

   Das Richtlinienprofil kann zur gleichen Richtlinie oder zu einer von Ihnen angegebenen Richtlinie kopiert werden.

5. Klicken Sie auf die Schaltfläche **Kopieren**.

Das Richtlinienprofil wird zur festgelegten Richtlinie kopiert. Dem zuletzt kopierten Profil wird die niedrigste Priorität zugewiesen. Wenn Sie das Profil zur selben Richtlinie kopieren, wird dem neu kopierten Profil der Index () angehängt, z. B. (1), (2).

Die Einstellungen des Profils, einschließlich Name und Priorität, können später geändert werden; das ursprüngliche Richtlinienprofil ändert sich in diesem Fall nicht.

Regeln für die Aktivierung des Richtlinienprofils erstellen

Um eine Regel für die Aktivierung des Richtlinienprofils zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Wählen Sie auf der Registerkarte **Richtlinienprofile** das Richtlinienprofil aus, für das Sie eine Aktivierungsregel anlegen möchten.

   Wenn die Richtlinienprofilliste leer ist, können Sie ein Richtlinienprofil erstellen.

3. Klicken Sie auf der Registerkarte **Aktivierungsregeln** auf die Schaltfläche **Hinzufügen**.

   Das Fenster mit Regeln für die Aktivierung des Richtlinienprofils wird geöffnet.

4. Geben Sie einen Namen für die Regel ein.

5. Aktivieren Sie die Kontrollkästchen neben den Bedingungen, die Einfluss auf die Aktivierung des erstellten Richtlinienprofils haben sollen:

   - **Allgemeine Regeln für die Aktivierung des Richtlinienprofils**

     Aktivieren Sie das Kontrollkästchen, um die Regeln für die Aktivierung des Richtlinienprofils auf dem Gerät je nach dem Zustand des autonomen Modus des Geräts, der Verbindungsregel des Geräts mit dem Administrationsserver und den dem Gerät zugewiesenen Tags anzupassen.

     Geben Sie für diese Option im nächsten Schritt Folgendes an:

     - **Gerätestatus**

       Legt die Bedingung für die Verfügbarkeit des Geräts im Netzwerk fest:

       - **Online** – Das Gerät befindet sich im Netzwerk und somit ist der Administrationsserver ist verfügbar.
       - **Autonom** – Das Gerät befindet sich in einem externen Netzwerk, daher ist der Administrationsserver nicht verfügbar.
       - **N/A** – Das Kriterium wird nicht angewendet.

     - **Netzwerkstandort des Geräts**

       Wählen Sie die Aktivierungsbedingung für das Richtlinienprofil (Regel wird erfüllt bzw. nicht erfüllt) und bestimmen Sie den Regelnamen.

       Die Regel definiert den Netzwerkstandort des Geräts für die Verbindung mit dem Administrationsserver; bei Erfüllen bzw. Nichterfüllen ihrer Bedingungen wird das Richtlinienprofil aktiviert.

       Die Beschreibung des Netzwerkstandorts der Geräte für die Verbindung mit dem Administrationsserver kann erstellt oder in der Regel für die Umschaltung des Administrationsagenten angepasst werden.

   - **Regeln für einen bestimmten Gerätebesitzer**

Geben Sie für diese Option im nächsten Schritt Folgendes an:

- **Gerätebesitzer**

  Aktivieren Sie die Option, um die Aktivierungsregel des Profils auf dem Gerät anhand des Geräteinhabers anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

  - Gerät gehört dem angegebenen Inhaber ("="-Symbol).
  - Gerät gehört nicht dem angegebenen Inhaber ("#"-Symbol).

    Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können den Gerätebesitzer angeben, wenn die Option aktiviert ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- **Gerätebesitzer gehört zu einer internen Sicherheitsgruppe**

  Aktivieren Sie die Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Zugehörigkeit des Geräteinhabers zur internen Sicherheitsgruppe von Kaspersky Security Center Linux anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

  - Der Gerätebesitzer gehört zur angegebenen Sicherheitsgruppe ("="-Symbol).
  - Der Gerätebesitzer gehört nicht zur angegebenen Sicherheitsgruppe ("#"-Symbol).

    Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können eine Sicherheitsgruppe für Kaspersky Security Center Linux angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- **Regeln für Hardware-Eigenschaften**

  Aktivieren Sie das Kontrollkästchen, um auf dem Gerät die Aktivierung der Richtlinienprofile je nach Speichergröße und Anzahl seiner logischen Prozesse anzupassen.

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  - **Größe des Arbeitsspeichers (MB)**

    Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Arbeitsspeichergröße des Geräts anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

    - Arbeitsspeicher des Geräts kleiner als festgelegter Wert (Zeichen "<")
    - Arbeitsspeicher des Geräts größer als festgelegter Wert (Zeichen ">")

    Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können die Größe des Arbeitsspeichers auf dem Gerät angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- **Anzahl der logischen Prozessoren**

  Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät anhand der Anzahl der logischen Prozessoren des Geräts anzupassen und zu aktivieren. In der Dropdown-Liste unter diesem Kontrollkästchen können die Kriterien für die Aktivierung des Profils ausgewählt werden:

  - Anzahl der logischen Prozesse des Geräts kleiner oder gleich festgelegter Wert (Zeichen "<")
  - Anzahl der logischen Prozesse des Geräts größer oder gleich festgelegter Wert (Zeichen ">")

  Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt. Sie können die Anzahl der logischen Prozessoren auf dem Gerät angeben. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

- **Regeln für zugeordnete Rollen**

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  - **Richtlinienprofil durch eine bestimmte Rolle des Gerätebesitzers aktivieren**

    Aktivieren Sie diese Option, um die Regel zur Aktivierung des Profils auf dem Gerät in Abhängigkeit von der Rolle des Besitzers zu konfigurieren. Fügen Sie die Rolle manuell aus der Liste vorhandener Rollen hinzu.

    Wenn die Option aktiviert ist, wird die Aktivierung des Profils auf dem Gerät abhängig von den festgelegten Kriterien durchgeführt.

- **Regeln für verwendete Tags**

  Aktivieren Sie das Kontrollkästchen, um die Regeln für die Aktivierung des Richtlinienprofils auf dem Gerät abhängig von den Tags anzupassen, die dem Gerät zugewiesen wurden. Sie können das Richtlinienprofil entweder für alle Geräte mit diesem Tag oder alle Geräte ohne dieses Tag aktivieren.

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  - **Liste der Tags**

    Geben Sie in der Liste der Tags Aktivierungsregeln für Geräte im Richtlinienprofil an, indem Sie die Kontrollkästchen der entsprechenden Tags aktivieren.

    Sie können neue Tags zur Liste hinzufügen, indem Sie diese im Feld über der Liste eingeben und auf die Schaltfläche **Hinzufügen** klicken.

    Das Richtlinienprofil erstreckt sich auf Geräte, in deren Beschreibung alle ausgewählten Tags vorkommen. Sind Kontrollkästchen deaktiviert, wird das Kriterium nicht angewandt. Standardmäßig sind die Kontrollkästchen deaktiviert.

  - **Gilt für Geräte ohne die angegebenen Tags**

    Aktivieren Sie die Option, wenn die Auswahl der Tags invertiert werden muss.

    Wenn diese Option aktiviert ist, werden Geräte, in deren Beschreibung keines der gewählten Tags vorkommt, in das Richtlinienprofil aufgenommen. Wenn diese Option deaktiviert ist, wird das Kriterium nicht angewendet.

    Diese Option ist standardmäßig deaktiviert.

- **Regeln für die Verwendung von Active Directory**

  Aktivieren Sie dieses Kontrollkästchen, um die Aktivierungsregeln für das Richtlinienprofil auf dem Gerät anzupassen. Die Regeln sind davon abhängig, ob das Gerät in einer Active Directory-Organisationseinheit (OU) vorhanden ist oder ob das Gerät (oder dessen Eigentümer) zu einer Active Directory-Sicherheitsgruppe gehört.

  Geben Sie für diese Option im nächsten Schritt Folgendes an:

  - **Mitgliedschaft des Gerätebesitzers in einer Active Directory-Sicherheitsgruppe**

    Bei aktivierter Option wird das Richtlinienprofil auf dem Gerät aktiviert, wenn dessen Inhaber Mitglied der angegebenen Sicherheitsgruppe ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

  - **Zugehörigkeit des Geräts zur Sicherheitsgruppe Active Directory**

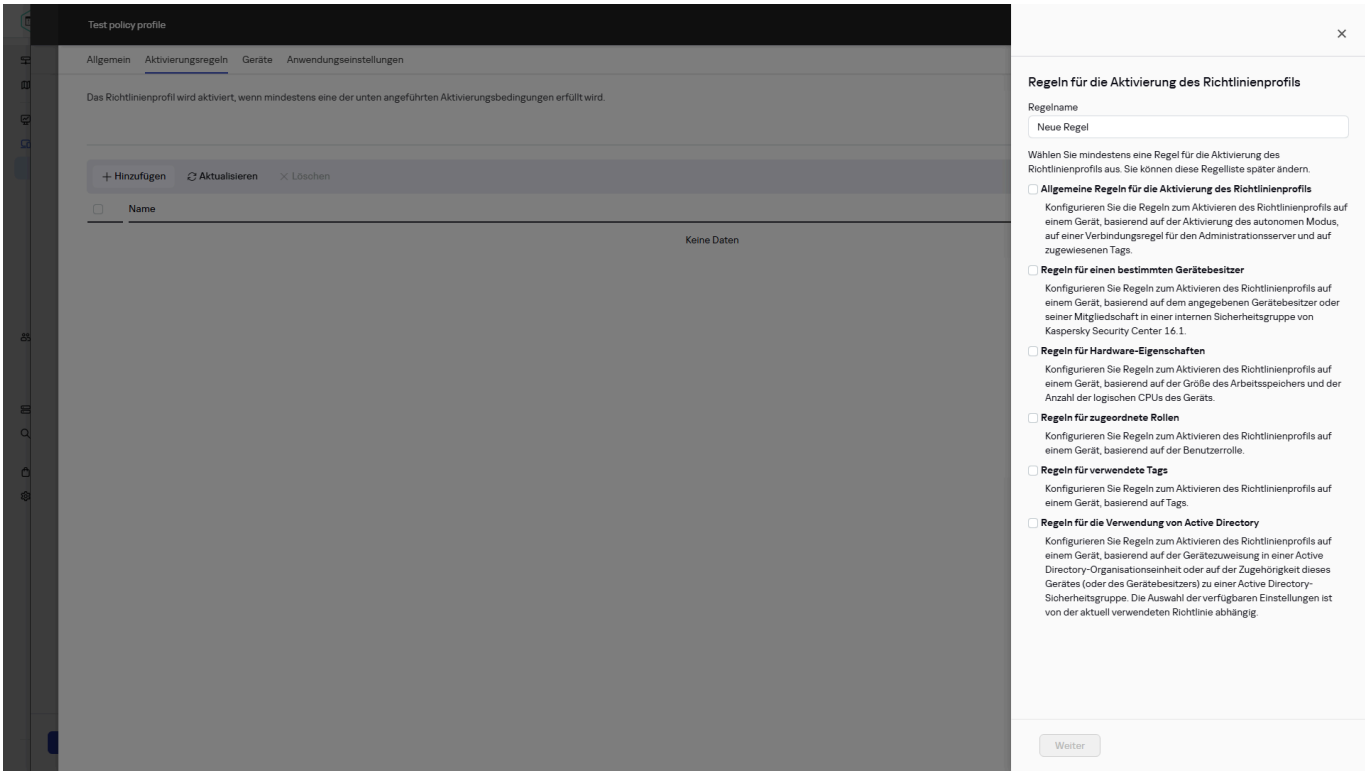
    Bei aktivierter Option wird das Richtlinienprofil auf dem Gerät aktiviert. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt. Diese Option ist standardmäßig deaktiviert.

  - **Gerätezuordnung in der Active Directory-Organisationseinheit**

    Bei aktivierter Option wird das Richtlinienprofil auf einem Gerät aktiviert, das explizit oder implizit in der angegebenen Active Directory-Organisationseinheit (OU) enthalten ist. Wenn die Option deaktiviert ist, wird das Aktivierungskriterium des Profils nicht angewandt.

    Diese Option ist standardmäßig deaktiviert.

Von der Auswahl der Einstellungen im ersten Schritt hängt die weitere Anzahl der Seiten des Assistenten ab. Sie können die Regeln für die Richtlinienprofilaktivierung später ändern.



Regeln für die Aktivierung des Richtlinienprofils erstellen

6. Überprüfen Sie die Liste der angepassten Einstellungen. Ist die Liste korrekt, klicken Sie auf **Erstellen**.

Das Profil wird gespeichert. Das Profil wird auf dem Gerät aktiviert, wenn die Aktivierungsregel ausgeführt wird.

Die Regeln für die Aktivierung des Richtlinienprofils, die für das Profil erstellt wurden, werden in den Eigenschaften des Richtlinienprofils auf der Registerkarte **Aktivierungsregeln** angezeigt. Sie können die Regel für die Aktivierung des Richtlinienprofils ändern oder löschen.

Mehrere Aktivierungsregeln können gleichzeitig ausgeführt werden.

Richtlinienprofil löschen

Um ein Richtlinienprofil zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Aktivieren Sie auf der Registerkarte **Richtlinienprofile** das Kontrollkästchen neben dem Richtlinienprofil, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.

3. Klicken Sie im folgenden Fenster erneut auf **Löschen**.

   Das Richtlinienprofil wird gelöscht. Wenn die Richtlinie von einer Gruppe einer niedrigeren Ebene geerbt wird, verbleibt das Profil in dieser Gruppe, wird aber zum Richtlinienprofil dieser Gruppe. Auf diese Weise werden wesentliche Veränderungen an den Einstellungen der verwalteten Anwendungen, die auf Geräten untergeordneter Gruppen installiert sind, unterbunden.

Richtlinienprofil exportieren und importieren

Sie können ein Richtlinienprofil in einer KLPROF-Datei speichern, ohne eine Richtlinie zu exportieren, und die KLPROF-Datei anschließend nutzen, um das gespeicherte Profil in die Richtlinie zu importieren.

Dadurch können Sie die Einstellungen des Richtlinienprofils schnell wiederherstellen, anstatt sie erneut konfigurieren zu müssen.

Ein Richtlinienprofil wird in die Richtlinie derselben Version der Anwendung importiert, aus der Sie das Profil exportiert haben. Für Anwendungen, welche die Abwärtskompatibilität von Richtlinien unterstützen (z. B. Kaspersky Endpoint Security für Windows), können Sie Richtlinienprofile in verschiedene Versionen der Richtlinie importieren.

So exportieren Sie ein Richtlinienprofil:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Wählen Sie auf der Registerkarte **Richtlinienprofile** das Richtlinienprofil aus, das Sie exportieren möchten.

3. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Exportieren**.

4. Geben Sie im neuen Fenster das Verzeichnis an, in dem Sie die Datei mit dem Richtlinienprofil speichern möchten.

   Bei Bedarf können Sie den Dateinamen ändern.

5. Klicken Sie auf **Speichern**.

Wenn der Vorgang erfolgreich abgeschlossen wurde, wird eine entsprechende Meldung auf dem Bildschirm angezeigt. Andernfalls wird eine Fehlermeldung angezeigt.

So importieren Sie ein Richtlinienprofil:

1. Wechseln Sie zu der Liste der Profile für die gewünschte Richtlinie.

   Daraufhin wird die Liste der Richtlinienprofile geöffnet.

2. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Importieren**.

3. Wählen Sie im neuen Fenster die KLPROF-Datei mit dem erforderlichen Richtlinienprofil und klicken Sie auf die Schaltfläche **Öffnen**.

   Die maximale Größe einer importierten Datei beträgt 4 MB.

Wenn der Vorgang erfolgreich abgeschlossen wurde, wird eine entsprechende Meldung auf dem Bildschirm angezeigt. Andernfalls wird eine Fehlermeldung angezeigt.

Das Richtlinienprofil wird mit dem Namen importiert, den es beim Export besaß, und nicht mit dem Namen der KLPROF-Datei.
Die Datei wird unabhängig davon, welche Priorität das Richtlinienprofil beim Export hatte, mit dem Status **Deaktiviert** und der niedrigsten Priorität importiert.

Der Import kann nicht durchgeführt werden:

- Wenn die Richtlinie bereits ein Profil mit demselben Namen besitzt.
- Wenn die Anzahl der Profile in der Richtlinie 100 beträgt.

Richtlinieneinstellungen des Administrationsagenten

Gehen Sie folgendermaßen vor, um die Richtlinieneinstellungen des Administrationsagenten anzupassen:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

2. Klicken Sie auf den Namen der Richtlinie für Administrationsagenten.

   Das Eigenschaftenfenster der Richtlinie des Administrationsagenten wird geöffnet. Das Eigenschaftenfenster enthält die im Folgenden beschriebenen Registerkarten und Einstellungen.

Der Vergleichstabelle können Sie im Detail entnehmen, wie die folgenden Einstellungen je nach verwendetem Betriebssystemtyp angewendet werden.

Allgemein

Auf dieser Registerkarte können Sie den Namen und Status der Richtlinie ändern und die Vererbung der Richtlinieneinstellungen anpassen:

- Im Feld **Name** können Sie den Namen der Richtlinie ändern.
- Im Block **Richtlinienstatus** können Sie einen der folgenden Richtlinienmodi auswählen:
  - **Aktiv**

    Bei Auswahl dieser Option wird die Richtlinie aktiv.

    Diese Variante ist standardmäßig ausgewählt.
  - **Inaktiv**

    Bei Auswahl dieser Option wird die Richtlinie inaktiv, aber im Ordner **Richtlinien** gespeichert. Bei Bedarf kann die Richtlinie aktiviert werden.
- In der Einstellungsgruppe **Vererbung von Einstellungen** können Sie Einstellungen für die Vererbung der Richtlinie anpassen:
  - **Einstellungen aus übergeordneter Richtlinie erben**

    Ist diese Option aktiviert, so werden die Werte der Richtlinieneinstellungen aus der Richtlinie der obersten Hierarchie-Ebene vererbt und können nicht geändert werden.

    Diese Option ist standardmäßig aktiviert.
  - **Vererbung der Einstellungen an untergeordnete Richtlinien erzwingen**

    Ist diese Option aktiviert, so werden die folgenden Aktionen ausgeführt, nachdem die Richtlinienänderungen übernommen wurden:
    - Einstellungen der Richtlinie werden in die Tochter-Richtlinien, d.h. in die Richtlinien der untergeordneten Administrationsgruppen, übertragen.
    - Im Block **Einstellungen erben** des Abschnitts **Allgemein** im Eigenschaftenfenster aller untergeordneten Richtlinien wird die Option **Einstellungen aus Richtlinie der höheren Ebene erben** automatisch aktiviert.

    Ist diese Option aktiviert, so können die Einstellungen der untergeordneten Richtlinien nicht geändert werden.

    Diese Option ist standardmäßig deaktiviert.

Konfiguration von Ereignissen

Auf dieser Registerkarte können Sie die Ereignisprotokollierung und die Benachrichtigung über Ereignisse konfigurieren. Die Ereignisse sind entsprechend ihrer Ereigniskategorien in folgenden Abschnitte eingeteilt:

- **Funktionsfehler**
- **Warnung**
- **Information**

Jeder Abschnitt enthält eine Liste mit Ereignistypen und der Standard-Speicherdauer des Ereignisses auf dem Administrationsserver (in Tagen). Nachdem Sie den Ereignistyps angeklickt haben, können Sie die Eigenschaften für die Protokollierung und die Benachrichtigung über die aus der Liste ausgewählten Ereignisse festgelegt werden. Standardmäßig werden die allgemeinen Benachrichtigungseinstellungen, die für den gesamten Administrationsserver festgelegt wurden, für alle Ereignistypen verwendet. Bestimmte Einstellungen können jedoch für die gewünschten Ereignistypen angepasst werden.

Sie können beispielsweise im Abschnitt **Warnung** den Ereignistyp **Es ist ein Sicherheitsproblem aufgetreten** konfigurieren. Solche Ereignisse können beispielsweise eintreten, wenn der freie Speicherplatz eines Verteilungspunkts weniger als 2GB beträgt (es sind mindestens 4 GB erforderlich, um Anwendungen remote zu installieren und Updates herunterzuladen). Um das Ereignis **Es ist ein Sicherheitsproblem aufgetreten** zu konfigurieren, klicken Sie es an und legen Sie fest, wo die aufgetretenen Ereignisse gespeichert werden sollen und wie über sie benachrichtigt werden soll.

Wenn der Administrationsagent einen Sicherheitsvorfall entdeckt hat, können Sie diesen Vorfall mithilfe der Einstellungen eines verwalteten Geräts verwalten.

Anwendungseinstellungen

Einstellungen

Im Abschnitt **Einstellungen** können Sie die Richtlinieneinstellungen des Administrationsagenten anpassen:

- **Dateien nur über Verteilungspunkte übertragen**

  Wenn diese Option aktiviert ist, beziehen die Administrationsagenten auf verwalteten Geräten die Updates ausschließlich von Verteilungspunkten.

  Wenn diese Option deaktiviert ist, beziehen die Administrationsagenten auf verwalteten Geräten die Updates von Verteilungspunkten oder vom Administrationsserver.

  Beachten Sie, dass die Sicherheitsanwendungen auf verwalteten Geräten die Updates aus der Quelle abrufen, die in der Update-Aufgabe für jede Sicherheitsanwendung festgelegt wurde. Wenn Sie die Option **Dateien nur über Verteilungspunkte übertragen** aktivieren, stellen Sie sicher, dass Kaspersky Security Center Linux in den Update-Aufgaben als Update-Quelle festgelegt ist.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Ereigniswarteschlange (MB)**

  In diesem Feld können Sie den maximalen Speicherplatz eingeben, welchen die Ereigniswarteschlange auf dem Laufwerk einnehmen kann.

  Standardmäßig ist der Wert auf 2 MB eingestellt.

- **Der Anwendung ist es erlaubt, auf dem Gerät erweiterte Daten über Richtlinien zu erfassen**

  Der Administrationsagent, der auf einem verwalteten Gerät installiert ist, überträgt Informationen über die angewendete Sicherheitsanwendungs-Richtlinie an die Sicherheitsanwendung (z. B. Kaspersky Endpoint Security für Linux). Die übertragenen Informationen können Sie auf der Benutzeroberfläche der Sicherheitsanwendung einsehen.

Der Administrationsagent überträgt die folgenden Informationen:

- Zeit, zu der die Richtlinie dem verwalteten Gerät zugestellt wurde.
- Name der aktiven Richtlinie zum Zeitpunkt der Übertragung der Richtlinien an das verwaltete Gerät.
- Name der Richtlinie für mobile Benutzer zum Zeitpunkt der Übertragung der Richtlinie an das verwaltete Gerät. (für den Administrationsagenten für Linux nicht verfügbar).
- Name und vollständiger Pfad der Administrationsgruppe, zu der das verwaltete Gerät gehörte, als die Richtlinie an das verwaltete Gerät zugestellt wurde.
- Liste der aktiven Richtlinienprofile mit ihren Namen und Prioritäten zum Zeitpunkt der Übertragung der Richtlinien an das verwaltete Gerät.

Sie können diese Informationen verwenden, um sicherzustellen, dass für das Gerät die richtige Richtlinie verwendet wird, und um Probleme zu lösen. Diese Option ist standardmäßig deaktiviert.

- **Dienst des Administrationsagenten vor unberechtigter Deinstallation und Beendigung schützen sowie Änderung der Einstellungen verhindern**

  Wenn diese Option aktiviert ist, kann nach der Installation des Administrationsagenten auf einem verwalteten Gerät die Komponente nicht ohne die entsprechenden Berechtigungen entfernt oder neu konfiguriert werden. Der Dienst des Administrationsagenten kann nicht beendet werden. Diese Option hat keine Auswirkung auf Domänencontroller.

  Aktivieren Sie diese Option, um den Administrationsagenten auf Workstations zu schützen, die mit lokalen Administratorrechten betrieben werden.

  Diese Option ist standardmäßig deaktiviert.

- **Deinstallationskennwort verwenden**

  Wenn diese Option aktiviert ist, können Sie durch das Anklicken der Schaltfläche **Ändern** auf Windows-Geräten das Kennwort für das Tool "klmover" und für die Aufgabe zur Remote-Deinstallation des Administrationsagenten angeben.

  Diese Option ist standardmäßig deaktiviert.

Datenverwaltung

Im Abschnitt **Datenverwaltung** können Sie die Objekttypen auswählen, deren Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen.

- **Details zu installierten Anwendungen**

  Ist diese Option aktiviert, werden auf den Administrationsserver Informationen über die auf den Client-Geräten installierten Anwendungen übertragen.

  Diese Option ist standardmäßig aktiviert.

- **Informationen über Patches einbinden**

  Informationen über die auf den Client-Geräten installierten Patches werden an den Administrationsserver übertragen. Das Aktivieren dieser Option kann die Auslastung des Administrationsservers und des DBMS erhöhen und eine Zunahme des Datenbankvolumens verursachen.

  Diese Option ist standardmäßig aktiviert. Sie ist nur für Windows verfügbar.

- **Informationen über Windows-Updates**

  Wenn diese Option aktiviert ist, werden an den Administrationsserver Informationen über erforderliche Microsoft Windows-Updates übertragen, die auf den Client-Geräten installiert werden müssen.

  Diese Option ist standardmäßig aktiviert. Sie ist nur für Windows verfügbar.

  Informationen über optionale Microsoft Windows-Updates werden nicht an den Administrationsserver übertragen.

- **Informationen über Schwachstellen in Programmen und entsprechende Updates**

  Wenn diese Option aktiviert ist, werden Informationen über Schwachstellen in Drittanbieter-Programmen (Software von Microsoft eingeschlossen), die auf verwalteten Geräten erkannt wurden, sowie Informationen über Programm-Updates zum Beheben der Drittanbieter-Schwachstellen (Software von Microsoft ausgeschlossen) an den Administrationsserver gesendet.

  Das Aktivieren der Option (**Informationen zu Schwachstellen in Programmen und entsprechenden Updates**) erhöht die Netzwerkbelastung, den Speicherbedarf des Administrationsservers und den Ressourcenverbrauch des Administrationsagenten.

  Diese Option ist standardmäßig aktiviert. Sie ist nur für Windows verfügbar.

  Um Updates für Software von Microsoft zu verwalten, verwenden Sie die Option **Informationen über Windows-Updates**.

- **Informationen über die Hardware-Inventur**

  Der auf einem Gerät installierte Administrationsagent sendet Informationen über die Geräte-Hardware an den Administrationsserver. Sie können die Hardware-Details in den Geräteeigenschaften anzeigen.

  Stellen Sie sicher, dass das Tool "lshw" auf den Linux-Geräten installiert ist, von denen Sie die Hardwaredetails abrufen möchten. Die von virtuellen Maschinen abgerufenen Hardwaredetails können je nach verwendetem Hypervisor unvollständig sein.

Wenn das Ändern der in diesem Abschnitt angegebenen Einstellungen in der Richtlinie des Administrationsagenten unterbunden ist, können Sie diese Einstellungen nicht ändern.

Software-Updates und Schwachstellen

Im Abschnitt **Software-Updates und Schwachstellen** können Sie die Untersuchung ausführbarer Dateien auf Schwachstellen aktivieren:

- **Ausführbare Dateien beim Start auf Schwachstellen untersuchen**

  Bei aktiviertem Kontrollkästchen werden ausführbare Dateien bei deren Start auf Schwachstellen untersucht.

  Diese Option ist standardmäßig aktiviert.

Verwaltung des Neustarts

Im Abschnitt **Verwaltung des Neustarts** können Sie die Aktion festlegen, die ausgeführt werden soll, wenn zur korrekten Ausführung, Installation oder Deinstallation des Programms ein Neustart des Betriebssystems des verwalteten Geräts erforderlich ist.

- **Betriebssystem nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für die Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

- **Betriebssystem bei Bedarf automatisch neu starten**

  Client-Geräte werden immer automatisch neu gestartet, wenn für das Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Variante ist standardmäßig ausgewählt.

  - **Aufforderung regelmäßig wiederholen nach (Min.)**

    Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer mit der festgelegten Häufigkeit auf, das Betriebssystem neu zu starten.

    Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

    Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

  - **Neustart erzwingen nach (Min.)**

    Nach der Aufforderung des Benutzers erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

    Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  - **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

    Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

    Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

    Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

Diese Option ist standardmäßig deaktiviert.

Verwaltung von Patches und Updates

Im Abschnitt Verwaltung von Patches und Updates können Sie das Abrufen und Verteilen der Updates sowie die Installation der Patches auf den verwalteten Geräten anpassen:

- **Anwendbare Updates und Patches für Komponenten mit dem Status "Nicht definiert" automatisch installieren**

  Ist diese Option aktiviert, so werden Kaspersky-Patches, die den Genehmigungsstatus *Nicht definiert* haben, sofort automatisch auf den verwalteten Geräten installiert, nachdem sie von den Update-Servern heruntergeladen wurden.

  Wenn die Option deaktiviert ist, werden die Patches von Kaspersky, die heruntergeladen und mit dem Status *Nicht festgestellt* markiert sind, erst installiert, wenn Sie ihren Status auf *Genehmigt* ändern.

  Diese Option ist standardmäßig aktiviert.

- **Updates und Antiviren-Datenbanken im Voraus vom Administrationsserver herunterladen (empfohlen)**

  Wenn diese Option aktiviert ist, wird das autonome Modell für das Abrufen von Updates verwendet. Wenn der Administrationsserver Updates empfängt, benachrichtigt der Administrationsagent (auf Geräten, auf denen er installiert ist) von den Updates, die für verwaltete Apps erforderlich sind. Wenn der Administrationsagent Informationen über diese Updates erhalten, ladet er die erforderlichen Dateien vom Administrationsserver im Voraus herunter. Bei der ersten Verbindung zum Administrationsagenten wird ein Updatedownload vom Administrationsserver initiiert. Nachdem der Administrationsagent alle Updates auf das Client-Gerät heruntergeladen hat, stehen die Updates den Programmen auf dem Gerät zur Verfügung.

  Wenn ein verwaltetes Programm auf dem Client-Gerät versucht, auf den Administrationsagenten zuzugreifen, um Updates herunterzuladen, überprüft der Administrationsagent, ob er über alle erforderlichen Updates verfügt. Wurden die Updates nicht mehr als 25 Stunden vor der Anfrage des verwalteten Programms vom Administrationsserver abgerufen, stellt der Administrationsagent keine Verbindung zum Administrationsserver her, sondern stellt dem verwalteten Programm die Updates aus dem lokalen Cache bereit. Eine Verbindung mit dem Administrationsserver wird möglicherweise nicht hergestellt, wenn der Administrationsagent Updates für Programme auf Client-Geräten bereitgestellt, für die Updates jedoch keine Verbindung erforderlich ist.

  Wenn diese Option deaktiviert ist, wird das autonome Modell für das Abrufen von Updates nicht verwendet. Updates werden gemäß dem Zeitplan der Aufgaben zum Update-Download verteilt.

  Diese Option ist standardmäßig aktiviert.

Konnektivität

Der Abschnitt **Konnektivität** enthält drei Unterabschnitte:

- **Netzwerk**
- **Verbindungsprofile**
- **Verbindungszeitplan**

Im Unterabschnitt **Netzwerk** können Sie die Einstellungen für die Verbindung zum Administrationsserver anpassen, die Nutzung eines UDP-Ports aktivieren und die Nummer des UDP-Ports festlegen.

- In der Einstellungsgruppe **Mit dem Administrationsserver verbinden** können Sie die Verbindungseinstellungen für den Administrationsserver anpassen und das Synchronisierungsintervall der Client-Geräte mit dem Administrationsserver festlegen:

  - **Synchronisierungsintervall (Min.)**

    Der Administrationsagent synchronisiert das verwaltete Gerät mit dem Administrationsserver. Es wird empfohlen, das Synchronisierungsintervall (auch als Herzschlag bezeichnet) auf 15 Minuten pro 10.000 verwaltete Geräte einzurichten.

    Bei einem Synchronisierungsintervall kleiner als 15 Minuten, wird die Synchronisierung alle 15 Minuten durchgeführt. Bei einem Synchronisierungsintervall größer gleich 15 Minuten, wird die Synchronisierung entsprechend des angegebenen Synchronisierungsintervalls durchgeführt.

  - **Netzwerkverkehr komprimieren**

    Aktivieren Sie diese Option, um die Geschwindigkeit der Datenübertragung durch den Administrationsagenten zu steigern, das Datenvolumen zu komprimieren und die Belastung für den Administrationsserver zu reduzieren.

    > Die CPU-Auslastung des Client-Computers kann ansteigen.

    Dieses Kontrollkästchen ist standardmäßig aktiviert.

  - **Ports des Administrationsagenten in der Windows-Firewall öffnen**

    Wenn diese Option aktiviert ist, werden die Ports, die für die Arbeit des Administrationsagenten erforderlich sind, zur Ausschlussliste der Microsoft Windows Firewall hinzugefügt.

    Diese Option ist standardmäßig aktiviert.

  - **SSL-Verbindung verwenden**

    Wenn diese Option aktiviert ist, erfolgt die Verbindung zum Administrationsserver über einen gesicherten Port mit SSL-Protokoll.

    Diese Option ist standardmäßig aktiviert.

  - **Verbindungs-Gateway auf einem Verteilungspunkt (falls vorhanden) mit den Standard-Verbindungseinstellungen verwenden**

    Wenn die Option aktiviert ist, wird das Verbindungs-Gateway auf dem Verteilungspunkt mit den Einstellungen verwendet, die in den Administrationsgruppeneigenschaften festgelegt sind.

    Diese Option ist standardmäßig aktiviert.

- **UDP-Port verwenden**

  Wenn es erforderlich ist, dass sich der Administrationsagent über einen UDP-Port mit dem Administrationsserver verbindet, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine **UDP-Portnummer** an. Diese Option ist standardmäßig aktiviert. Der standardmäßige UDP-Port für die Verbindung zum Administrationsserver ist 15000.

- **UDP-Port**

  Im Eingabefeld können Sie die Nummer des UDP-Ports eingeben. Standardmäßig wird Portnummer 15000 verwendet.

  Für die Eingabe wird das Dezimalformat verwendet.

- **Verteilungspunkt verwenden, um eine Verbindung mit dem Administrationsserver zu erzwingen**

  Wählen Sie diese Option, wenn Sie im Fenster mit den Einstellungen des Verteilungspunktes die Option **Diesen Verteilungspunkt als Push-Server verwenden** ausgewählt haben. Andernfalls wird der Verteilungspunkt nicht als Push-Server fungieren.

Im Unterabschnitt **Verbindungsprofile** können Sie die Einstellungen des Netzwerkstandortes festlegen und den Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist:

- **Einstellungen des Netzwerkstandorts**

  Die Einstellungen des Netzwerkspeicherorts bestimmen die Merkmale des Netzwerks, mit dem das Client-Gerät verbunden ist, und legen die Regeln für den Wechsel des Administrationsagenten von einem Administrationsserver-Verbindungsprofil zu einem anderen fest (im Falle sich ändernder Merkmale des Netzwerks).

- **Verbindungsprofile des Administrationsservers**

  Sie können ein Profil für die Verbindung des Administrationsagenten mit dem Administrationsserver anzeigen und hinzufügen. In diesem Abschnitt können ferner die Umschaltregeln des Administrationsagenten auf andere Administrationsserver im Fall des Auftretens folgender Ereignisse festgelegt werden:

  - Verbindung des Client-Geräts mit einem anderen lokalen Netzwerk.
  - Trennung der Verbindung des Geräts vom lokalen Unternehmensnetzwerk.
  - Änderung der Verbindungs-Gateway-Adresse oder der Adresse des DNS-Servers.

- **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist**

  Wenn diese Option aktiviert ist, und eine Verbindung über dieses Profil besteht, verwenden Anwendungen, die auf dem Client-Gerät installiert sind, Richtlinienprofile für Geräte im Modus für mobile Benutzer sowie Richtlinien für mobile Benutzer. Wurde für die Anwendung keine Richtlinie für mobile Benutzer definiert, verwendet die Anwendung die aktive Richtlinie.

  Wenn diese Option deaktiviert ist, wenden die Anwendungen die aktiven Richtlinien an.

  Diese Option ist standardmäßig deaktiviert.

Im Unterabschnitt **Verbindungszeitplan** können Sie Zeitintervalle festlegen, in denen der Administrationsagent Daten auf den Administrationsserver übertragen soll:

- **Verbindung bei Bedarf herstellen**

  Bei dieser Variante wird eine Verbindung dann hergestellt, wenn Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen.

  Diese Variante ist standardmäßig ausgewählt.

- **Verbindung in den angegebenen Zeiträumen herstellen**

  Bei dieser Variante wird eine Verbindung des Administrationsagenten mit dem Administrationsserver in den vorgegebenen Zeiträumen hergestellt. Sie können mehrere Zeiträume für die Verbindung hinzufügen.

Netzwerkabfrage durch Verteilungspunkte

Im Abschnitt **Netzwerkabfrage durch Verteilungspunkte** können Sie die automatische Abfrage des Netzwerks anpassen. Sie können die folgenden Optionen verwenden, um die Abfrage zu aktivieren und ihre Häufigkeit festzulegen:

- **Windows-Netzwerk**

  Diese Option ist nur für Windows-basierte Verteilungspunkte verfügbar.

  Wenn diese Option aktiviert ist, fragt der Administrationsserver das Netzwerk automatisch gemäß dem Zeitplan ab, den Sie über die Links **Zeitplan für schnelle Abfrage festlegen** und **Zeitplan für vollständige Abfrage festlegen** eingerichtet haben.

  Wenn diese Option deaktiviert ist, fragt der Administrationsserver das Netzwerk mit jenem Intervall ab, das im Feld **Intervall für Netzwerkabfragen (Min.)** angegeben ist.

  Das Intervall der Gerätesuche kann für Versionen des Administrationsagenten in den Feldern **Intervall für Abfrage von Windows-Domänen (Min.)** (für schnelle Abfragen eines Windows-Netzwerks) und **Intervall für Netzwerkabfragen (Min.)** (für vollständige Abfragen eines Windows-Netzwerks) angepasst werden.

  Diese Option ist standardmäßig deaktiviert.

- **IP-Bereiche**

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt die IP-Bereiche automatisch gemäß dem Zeitplan ab, den Sie über die Schaltfläche **Abfragezeitplan festlegen** eingerichtet haben.

  Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt keine IP-Bereiche ab.

  Das Intervall der Abfrage des IP-Bereichs kann für Versionen des Administrationsagenten bis Version 10.2 im Feld **Abfrageintervall (Min.)** eingestellt werden. Der Abschnitt ist verfügbar, wenn die Option aktiviert ist.

  Diese Option ist standardmäßig deaktiviert.

- **Zeroconf**

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt das Netzwerk mit IPv6-Geräten unter Verwendung von Zero-configuration Networking (auch als *Zeroconf* bezeichnet) automatisch ab. In diesem Fall werden aktivierte IP-Bereichsabfragen ignoriert, da der Verteilungspunkt das gesamte Netzwerk abfragt.

  Um Zeroconf verwenden zu können, müssen die folgenden Bedingungen erfüllt sein:

  - Der Verteilungspunkt muss unter Linux laufen.
  - Sie müssen auf dem Verteilungspunkt das Tool "avahi-browse" installieren.

  Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt Netzwerke mit IPv6-Geräten nicht ab.

  Diese Option ist standardmäßig deaktiviert.

- **Domänencontroller**

  Wenn diese Option aktiviert ist, fragt der Verteilungspunkt die Domänencontroller automatisch gemäß dem Zeitplan ab, den Sie über die Schaltfläche **Abfragezeitplan festlegen** eingerichtet haben.

  Wenn diese Option deaktiviert ist, fragt der Verteilungspunkt keine Domänencontroller ab.

  Das Intervall für die Abfrage des Domänencontrollers kann für Administrationsagenten bis Version 10.2 im Feld **Abfrageintervall (Min.)** eingestellt werden. Der Feld ist verfügbar, wenn diese Option aktiviert ist.

  Diese Option ist standardmäßig deaktiviert.

Netzwerk-Einstellungen für Verteilungspunkte

Im Abschnitt **Netzwerk-Einstellungen für Verteilungspunkte** können Sie die Einstellungen für den Internetzugang festlegen:

- **Proxyserver verwenden**
- **Adresse**
- **Port**
- **Proxyserver für lokale Adressen umgehen**

  Wenn die Option aktiviert ist, wird bei der Verbindung mit den Geräten im lokalen Netzwerk kein Proxyserver verwendet.

  Diese Option ist standardmäßig deaktiviert.

- **Authentifizierung am Proxyserver**

  Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

KSN-Proxy (Verteilungspunkte)

Im Abschnitt **KSN-Proxy (Verteilungspunkte)** können Sie die Anwendung anpassen, um den Verteilungspunkt zum Weiterleiten von Anfragen des Kaspersky Security Network (KSN) von den verwalteten Geräten zu verwenden:

- **KSN-Proxy auf dem Verteilungspunkt aktivieren**

  Der KSN-Proxy-Service wird auf dem Gerät ausgeführt, das als Verteilungspunkt verwendet wird. Verwenden Sie diese Funktion, um Datenverkehr im Netzwerk neu zu verteilen und zu optimieren.

  Der Verteilungspunkt sendet die KSN-Statistik, die in der Erklärung zu Kaspersky Security Network aufgeführt sind, an Kaspersky.

  Diese Option ist standardmäßig deaktiviert. Die Aktivierung dieser Option wird erst wirksam, wenn im Fenster mit den Eigenschaften des Administrationsservers die Optionen **Administrationsserver als Proxyserver verwenden** und **Ich akzeptiere die Nutzungsbedingungen von Kaspersky Security Network** aktiviert sind.

  Sie können dem Knoten eines aktiv-passiven Clusters die Rolle als Verteilungspunkt zuweisen und den KSN-Proxyserver auf diesem Knoten aktivieren.

- **KSN-Anfragen an den Administrationsserver weiterleiten**

  Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an den Administrationsserver weiter.

  Diese Option ist standardmäßig aktiviert.

- **Direkt über das Internet auf KSN Cloud/KPSN zugreifen**

  Der Verteilungspunkt leitet KSN-Anfragen von den verwalteten Geräten an die KSN Cloud oder an KPSN weiter. KSN-Anfragen, die der Verteilungspunkt selbst generiert, werden ebenso direkt an KSN Cloud oder KPSN gesendet.

- **TCP-Port**

  Die Nummer des TCP-Ports, den die verwalteten Geräte verwenden werden, um eine Verbindung mit dem KSN-Proxyserver herzustellen. Standardmäßig wird Portnummer 13111 verwendet.

- **UDP-Port**

  Wenn es erforderlich ist, dass sich der Administrationsagent über einen UDP-Port mit dem Administrationsserver verbindet, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine **UDP-Portnummer** an. Diese Option ist standardmäßig aktiviert. Der standardmäßige UDP-Port für die Verbindung zum Administrationsserver ist 15000.

- **HTTPS-Port**

  Wenn die verwalteten Geräte eine Verbindung mit dem KSN-Proxyserver über einen HTTPS-Port herstellen sollen, aktivieren Sie die Option **HTTPS verwenden** und geben Sie anschließend im Feld **HTTPS-Port** eine Portnummer an. Diese Option ist standardmäßig deaktiviert. Der standardmäßige HTTPS-Port für die Verbindung zum KSN-Proxyserver ist 17111.

Updates (Verteilungspunkte)

Sie können die Funktion zum Download von diff-Dateien im Abschnitt **Updates (Verteilungspunkte)** aktivieren, damit die Verteilungspunkte die Updates in Form von diff-Dateien von den Kaspersky-Update-Servern erhalten.

Verwaltung lokaler Benutzerkonten (nur Linux)

Der Abschnitt **Verwaltung lokaler Benutzerkonten (nur Linux)** enthält drei Unterabschnitte:

- **Verwaltung von Benutzerzertifikaten**
- **Anwendbare lokale Administrationsgruppen hinzufügen oder bearbeiten**
- **Referenzdatei hochladen, um die sudoers-Datei auf dem Benutzergerät vor Änderungen zu schützen**

Im Unterabschnitt **Verwaltung von Benutzerzertifikaten** können Sie angeben, welche Stammzertifikate installiert werden sollen. Diese Zertifikate können beispielsweise verwendet werden, um die Authentizität von Websites oder Webservern zu überprüfen.

- **Root-Zertifikate installieren**

  Wenn diese Option aktiviert ist, werden die zur Tabelle hinzugefügten Zertifikate auf den angegebenen Geräten installiert.

  Wenn diese Option deaktiviert ist, werden auf den angegebenen Geräten keine Zertifikate installiert.

  Diese Option ist standardmäßig deaktiviert.

- **Hinzufügen**

  Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie ein Zertifikat hinzufügen können.

  Das Zertifikat muss kleiner als 10 MB sein.

  Kaspersky Security Center unterstützt Zertifikate mit folgenden Erweiterungen: cer, crt, cert, pem und key.

Im Unterabschnitt **Anwendbare lokale Administrationsgruppen hinzufügen oder bearbeiten** können Sie die Gruppen mit lokalen Administratoren verwalten. Diese Gruppen werden beispielsweise verwendet, wenn lokale Administratorrechte entzogen werden. Sie können die Liste der privilegierten Benutzerkonten auch mithilfe des **Bericht über privilegierte Gerätenutzer (nur Linux)** überprüfen.

- **Hinzufügen**

  Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie eine Gruppe mit lokalen Administratoren hinzufügen können.

- **Bearbeiten**

  Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie die Gruppe mit lokalen Administratoren bearbeiten können.

  Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben der Gruppe mit lokalen Administratoren aktiviert ist.

- **Löschen**

  Mit dieser Schaltfläche wird die ausgewählte Gruppe mit lokalen Administratoren aus der Tabelle gelöscht.

  Diese Schaltfläche ist verfügbar, wenn das Kontrollkästchen neben der Gruppe mit lokalen Administratoren aktiviert ist.

Im Unterabschnitt **Referenzdatei hochladen, um die sudoers-Datei auf dem Benutzergerät vor Änderungen zu schützen**, können Sie die Kontrolle der sudoers-Datei anpassen. Privilegierte Gruppen und Gerätebenutzer werden durch die sudoers-Datei auf dem Gerät definiert. Die sudoers-Datei befindet sich unter `/etc/sudoers`. Sie können eine sudoers-Referenzdatei hochladen, um die eigentliche sudoers-Datei vor Änderungen zu schützen. Dadurch werden unerwünschte Änderungen an der sudoers-Datei verhindert.

Eine ungültige sudoers-Referenzdatei kann zu Fehlfunktionen auf dem Gerät des Benutzers führen.

- **sudoers-Datei überwachen**

  Wenn diese Option aktiviert ist, wird die sudoers-Datei durch die aktuelle -sudoers-Referenzdatei ersetzt.

  Wenn diese Option deaktiviert ist, bleibt die sudoers-Datei unverändert.

  Diese Option ist standardmäßig deaktiviert.

- **sudoer-Referenzdatei**

  In diesem Feld wird der Name der hochgeladenen sudoers-Referenzdatei angezeigt.

- **Hochladen**

  Mit dieser Schaltfläche wird ein Fenster geöffnet, in dem Sie sudoers-Referenzdatei können.

- **Aktuelle sudoers-Referenzdatei**

  Wenn Sie auf diese Schaltfläche klicken, wird der Inhalt der aktuellen sudoers-Datei angezeigt.

Revisionsverlauf

Auf der Registerkarte **Revisionsverlauf** können Sie:

- Den Verlauf der Richtlinienrevisionen anzeigen und speichern.
- Einen Rollback auf eine Richtlinienrevision durchführen.
- Beschreibungen von Richtlinienrevisionen hinzufügen und bearbeiten.
- Richtlinienrevisionen vergleichen.

Administrationsagent für Windows, Linux und macOS: Vergleich

Die Verwendung des Administrationsagenten hängt vom Betriebssystem des Geräts ab. Die Einstellungen für die Richtlinie des Administrationsagenten und das Installationspaket unterscheiden sich ebenfalls in Abhängigkeit vom Betriebssystem. In der folgenden Tabelle werden für den Administrationsagenten die Funktionen und Verwendungsszenarien für Windows-, Linux-und macOS-Betriebssysteme verglichen.

Vergleich der Funktionen des Administrationsagenten

Funktion des Administrationsagenten	Windows	Linux	macOS
Installation			
Installation mittels Klonen eines Festplatten-Images mit Betriebssystem und installiertem Administrationsagenten unter Verwendung von Drittanbieter-Tools	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	✓	✓
Installation mittels Drittanbietern-Tools zur Remote-Installation von Anwendungen	✓	✓	✓
Installation durch manuelles Starten der Installer der Anwendungen auf den Geräten	✓	✓	✓
Installation des Administrationsagenten im Silent-Modus	✓	✓	✓
Client-Gerät manuell mit Administrationsserver verbinden. "klmover"-Tool	✓	✓	✓
Automatischen Installation von Updates und Patches für die Komponenten von Kaspersky Security Center	✓	✓	–
Automatische Verteilung von Schlüsseln	✓	✓	✓
Erzwungene Synchronisierung	✓	✓	✓ Außer Push-Server
Verteilungspunkt			

Funktion des Administrationsagenten	Windows	Linux	macOS
Verwendung als Verteilungspunkt	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	✓	✓
Berechnung der Anzahl und Konfiguration der Verteilungspunkte	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	✓ Ohne die Verwendung von Network Location Awareness (NLA).	✓ Ohne die Verwendung von Network Location Awareness (NLA).
Autonomes Modell für den Download von Updates	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	✓	✓
Netzwerkabfrage	✓ • IP-Bereiche abfragen • Abfrage des Domänencontrollers (Microsoft Active Directory) Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	✓ IP-Bereiche abfragen Zeroconf-Abfrage Abfrage des Domänencontrollers (Microsoft Active Directory, Samba 4 Active Directory)	–
KSN-Proxy-Service auf dem Verteilungspunkt ausführen	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	✓	–
Herunterladen von Updates über Kaspersky-Update-Server in die Datenverwaltungen der Verteilungspunkte, welche wiederum die Updates an verwaltete Geräte verteilen	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	✓	– (Wenn ein oder mehrere Geräte, die unter Linux oder macOS laufen, in den Bereich der Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte fallen, schließt die Aufgabe mit dem Status "Fehlgeschlagen" ab, selbst wenn sie auf allen Windows-Geräten erfolgreich abgeschlossen wurde)
Push-Installation von Anwendungen	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	Eingeschränkt: Es ist nicht möglich, mithilfe von Linux-Verteilungspunkten eine Push-Installation auf Windows-Geräten durchzuführen.	Eingeschränkt: Es ist nicht möglich, mithilfe von macOS-Verteilungspunkten eine Push-Installation auf Windows-Geräten durchzuführen.
Verwendung als Push-Server	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	✓	–
Umgang mit Drittanbieter-Anwendungen			
Remote-Installation von Anwendungen auf Geräten	✓	✓	✓ Weitere Informationen finden Sie im folgenden Artikel: Remote-Installation von Anwendungen auf macOS-Geräten.
Anpassen von Updates des Betriebssystems in einer Richtlinie des Administrationsagenten	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	–	–

Funktion des Administrationsagenten	Windows	Linux	macOS
Informationen über Schwachstellen in Programmen anzeigen	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	–	–
Schwachstellensuche in Anwendungen	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	–	–
Programm-Updates	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	–	–
Inventarisierung von auf Geräten installierten Programmen	✓	✓	–
Virtuelle Maschinen			
Installation des Administrationsagenten auf einer virtuellen Maschine	✓	✓	✓
Einstellungen für Optimierung der Virtual Desktop Infrastructure (VDI)	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	✓	✓
Unterstützung von dynamischen virtuellen Maschinen	✓ Einschränkung: Wird vom Administrationsagent für Microsoft Windows on ARM nicht unterstützt.	✓	✓
Anderes			
Audit von Aktionen auf einem Remote-Client-Gerät mithilfe der Windows Desktopfreigabe	✓	–	–
Überwachung des Status des Antiviren-Schutzes	✓	✓	✓
Verwaltung von Geräteneustarts	✓	–	–
Unterstützung von Rollbacks des Dateisystems	✓	✓	✓
Verwendung eines Administrationsagenten als Verbindungs-Gateway	✓	✓	✓
Verbindungsmanager	✓	✓	✓
Verbindungsprofile für mobile Benutzer	✓	✓	✓
Wechsel des Administrationsagenten von einem Administrationsserver auf einen anderen (automatisch nach Netzwerkstandort)	✓	✓	✓
Verbindung des Client-Geräts mit dem Administrationsserver prüfen. "klnagchk"-Tool	✓	✓	✓

Funktion des Administrationsagenten	Windows	Linux	macOS
Remotedesktopverbindung mit dem Client-Gerät herstellen	✓	✓	✓ Unter Verwendung des Virtual Network Computing-Systems (VNC).
Herunterladen eines autonomen Installationspaketes mithilfe des Migrationsassistenten	✓	✓	✓
Anzeigen von Informationen über die Hardware von Client-Geräten	✓	✓ Informationen über die Hardware von Linux-Geräten, die von den darauf installierten Administrationsagenten an den Administrationsserver gesendet werden, sind auf die in der Beschreibung Einstellungen des verwalteten Geräts angegeben Informationen eingeschränkt.	✓ Informationen über die Hardware von macOS-Geräten, die von den darauf installierten Administrationsagenten an den Administrationsserver gesendet werden, sind auf die in der Beschreibung Einstellungen des verwalteten Geräts angegeben Informationen eingeschränkt.

Vergleich der Einstellungen des Administrationsagenten nach Betriebssystemen

Die folgende Tabelle stellt eine Übersicht über die verfügbaren Einstellungen der Richtlinie des Administrationsagenten in Abhängigkeit des Betriebssystems von dem Gerät dar, auf dem der Administrationsagent installiert ist.

Einstellungen des Administrationsagenten: Vergleich nach Betriebssystemen

Abschnitt Einstellungen	Windows	Linux	macOS
Allgemein	✓	✓	✓
Konfiguration von Ereignissen	✓	✓	✓
Einstellungen	✓	✓ Es sind folgende Optionen verfügbar: • **Dateien nur über Verteilungspunkte übertragen** • **Maximale Größe der Ereigniswarteschlange (MB)** • **Der Anwendung ist es erlaubt, auf dem Gerät erweiterte Daten über Richtlinien zu erfassen**	✓
Datenverwaltung	✓	✓ Es sind folgende Optionen verfügbar: • **Details zu installierten Anwendungen** • **Informationen über die Hardware-Inventur**	✓ Die Option **Informationen über das Hardware-Register** ist verfügbar.
Konnektivität → Netzwerk	✓	✓ Mit Ausnahme der Option **Ports des Administrationsagenten in der Windows-Firewall öffnen**.	✓
Konnektivität → Verbindungsprofile	✓	✓	✓

Abschnitt Einstellungen	Windows	Linux	macOS
Konnektivität → Verbindungszeitplan	✓	✓	✓
Netzwerkabfrage durch Verteilungspunkte	✓ Es sind folgende Optionen verfügbar: • **Windows-Netzwerk** • **IP-Bereiche** • **Domänencontroller**	✓ Es sind folgende Optionen verfügbar: • **Zeroconf** • **IP-Bereiche** • **Domänencontroller**	–
Netzwerk-Einstellungen für Verteilungspunkte	✓	✓	✓
KSN-Proxy (Verteilungspunkte)	✓	✓	–
Updates (Verteilungspunkte)	✓	✓	–
Revisionsverlauf	✓	✓	✓

Modus für geringem Ressourcenverbrauch des Administrationsagenten aktivieren und deaktivieren

Im ressourcenschonenden Modus können Sie auf dem Client-Gerät die Auslastung des Arbeitsspeichers durch den installierten Administrationsagenten einschränken. Der ressourcenschonende Modus ist standardmäßig deaktiviert.

Im ressourcenschonenden Modus werden die folgenden Funktionen nicht ausgeführt:

- Der Administrationsagent kann nicht als Verteilungspunkt zugewiesen werden (weder manuell noch automatisch).
- Der Administrationsagent protokolliert keine Informationen über den Status des Administrationsagenten in einer separaten Textdatei.
- Der Administrationsagent unterstützt das Offline-Modell für Update-Downloads nicht.
- Die folgenden Komponenten und Prozesse sind deaktiviert:
  - Abrufen von Informationen über Drittanbieter-Updates und Schwachstellen.
  - Ausführen des KSN Proxy auf dem Verteilungspunkt.
  - Hochladen von Updates in die Datenverwaltung des Verteilungspunkts.
  - Umgehen der DNS-Server-Sperre.
  - Abrufen von Informationen über freien Speicherplatz.

Wenn der ressourcenschonende Modus deaktiviert wird, werden die Komponenten und Prozesse wieder ausgeführt.

So aktivieren Sie den ressourcenschonenden Modus:

1. Führen Sie in der Befehlszeile den folgenden Befehl aus:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Starten Sie den Administrationsagenten mithilfe des folgenden Befehls neu:

   ```
   sudo service klnagent64 restart
   ```

3. Überprüfen Sie im Protokoll des Betriebssystems, ob der folgende Eintrag angezeigt wird: **Kaspersky Security Center Administrationsagent wird im Modus für geringen Ressourcenverbrauch ausgeführt**.

Der ressourcenschonende Modus ist aktiviert.

So deaktivieren Sie den ressourcenschonenden Modus:

1. Führen Sie in der Befehlszeile den folgenden Befehl aus:

   ```
   sudo /opt/kaspersky/klnagent64/sbin/klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Starten Sie den Administrationsagenten mithilfe des folgenden Befehls neu:

   ```
   sudo service klnagent64 restart
   ```

Der ressourcenschonende Modus ist deaktiviert.

Sie können den Modus für geringem Ressourcenverbrauch auch remote aktivieren, indem Sie die Aufgabe *Remote-Ausführung von Skripten* verwenden.

Konfigurieren der Schutzeinstellungen für verwaltete Anwendungen

Zum Konfigurieren der Schutzeinstellungen für verwaltete Kaspersky-Anwendungen können Sie Richtlinien verwenden.

Weitere Informationen zum Konfigurieren von Richtlinien für Kaspersky Endpoint Security finden Sie in den entsprechenden Hilfen:

- Hilfe zu Kaspersky Endpoint Security für Windows
- Hilfe zu Kaspersky Endpoint Security für Linux
- Hilfe zu Kaspersky Endpoint Security for Mac

Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren

Der optimale und empfohlene Zeitplan für Kaspersky Endpoint Security ist **Nach dem Download neuer Updates in die Datenverwaltung**, wenn das Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** aktiviert ist.

Manuelle Konfiguration der Gruppenaufgabe zur Untersuchung des Geräts durch Kaspersky Endpoint Security

Der Schnellstartassistent erstellt die Gruppenaufgabe zur Untersuchung des Geräts. Wenn der automatisch festgelegte Zeitplan für die Gruppenaufgabe zur Untersuchung für Ihr Unternehmen ungeeignet ist, müssen Sie den für diese Aufgabe am besten geeigneten Zeitplan basierend auf den im Unternehmen festgelegten Arbeitsplatzregeln manuell festlegen.

So ist beispielsweise ist für die Aufgabe der Zeitplan **Freitags um 19:00 Uhr starten** mit automatischer zufälliger Streuung ausgewählt und das Kontrollkästchen **Übersprungene Aufgaben starten** ist deaktiviert. Wenn in diesem Fall die Geräte des Unternehmens freitags, um 18:30 Uhr heruntergefahren werden, bedeutet dies, dass die Untersuchungsaufgabe des Geräts niemals ausgeführt wird. In diesem Fall müssen Sie die Gruppenaufgabe zur Untersuchung manuell einrichten.

Kaspersky Security Network (KSN)

In diesem Abschnitt wird die Verwendung der Infrastruktur der Online-Dienste von Kaspersky Security Network (KSN) beschrieben. Er enthält Informationen über KSN sowie Anleitungen zur Aktivierung von KSN, zur Konfiguration des Zugriffs auf KSN und über die Statistiken der Verwendung des KSN-Proxyservers.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Über KSN

Das Kaspersky Security Network (KSN) ist eine Infrastruktur von Online-Diensten, die Zugriff auf die aktuelle Wissensdatenbank von Kaspersky bietet, in der Informationen über die Reputation der Dateien, Web-Ressourcen und Programme enthalten sind. Die Nutzung der Daten aus dem Kaspersky Security Network gewährleistet eine höhere Reaktionsschnelligkeit der Kaspersky-Programme auf Bedrohungen, erhöht die Effektivität vieler Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen. Mit KSN können aus den Kaspersky-Reputations-Datenbanken Informationen über die Anwendungen abgerufen werden, die auf den verwalteten Geräten installiert sind.

Mit der Teilnahme an KSN stimmen Sie zu, dass Informationen über die Ausführung der auf den Client-Geräten installierten Kaspersky-Anwendungen, die von Kaspersky Security Center Linux verwaltet werden, automatisch an Kaspersky übertragen werden. Die Übertragung von Informationen erfolgt gemäß den aktuellen Einstellungen für den Zugriff auf KSN.

Kaspersky Security Center Linux unterstützt die folgenden KSN-Infrastrukturlösungen:

- *Global KSN* ist eine Lösung, mit der Sie Informationen mit dem Kaspersky Security Network austauschen können. Wenn Sie an KSN teilnehmen, stimmen Sie zu, dass Informationen über die Ausführung der auf den Client-Geräten installierten Kaspersky-Anwendungen, die von Kaspersky Security Center Linux verwaltet werden, automatisch an Kaspersky übertragen werden. Die Übertragung von Informationen erfolgt gemäß den aktuellen Einstellungen für den Zugriff auf KSN. Kaspersky-Analysten analysieren zusätzlich erhaltene Informationen und nehmen sie in die Reputations- und Statistikdatenbanken von Kaspersky Security Network auf. Kaspersky Security Center Linux verwendet diese Lösung standardmäßig.

- *Kaspersky Private Security Network (KPSN)* ist eine Lösung, die es Benutzern von Geräten mit installierten Kaspersky-Anwendungen ermöglicht, Zugriff auf die Reputationsdatenbanken von Kaspersky Security Network und andere statistische Daten zu erhalten, ohne Daten von ihren eigenen Geräten an Global KSN zu senden. KPSN richtet sich an Unternehmenskunden, die aus einem der folgenden Gründe nicht an Kaspersky Security Network teilnehmen können:

  - Die Benutzergeräte haben keine Internetverbindung.

  - Die Übermittlung von Daten an einen Punkt außerhalb des Landes oder außerhalb des lokalen Unternehmensnetzwerks ist gesetzlich oder aufgrund von Sicherheitsrichtlinien des Unternehmens untersagt.

  Sie können die Zugriffseinstellungen von Kaspersky Private Security Network im Abschnitt **KSN-Proxy** des Eigenschaftenfensters des Administrationsservers einstellen.

Die Programm fordert Sie auf, während der Ausführung des Schnellstartassistenten eine Verbindung zu KSN herzustellen. Sie können während der Ausführung des Programms jederzeit mit der Verwendung von KSN beginnen oder auf KSN verzichten.

Sie verwenden KSN gemäß der KSN-Erklärung, die Sie lesen und akzeptieren, wenn Sie KSN aktivieren. Wird die KSN-Erklärung aktualisiert, so wird sie Ihnen bei einem Upgrade der Version des Administrationsservers angezeigt. Sie können die aktualisierte KSN-Erklärung akzeptieren oder ablehnen. Wenn Sie diese ablehnen, verwenden Sie KSN weiterhin gemäß der vorherigen Version der KSN-Erklärung, die Sie zuvor akzeptiert haben.

Bei aktiviertem KSN überprüft Kaspersky Security Center Linux, ob die KSN-Server erreichbar sind, um das Einhalten des Sicherheitsniveaus für die verwalteten Geräte zu gewährleisten. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet die Anwendung öffentliche DNS-Server.

Vom Administrationsserver verwaltete Client-Geräte interagieren mithilfe des KSN-Proxyservers mit KSN. Der KSN-Proxyserver bietet folgende Möglichkeiten:

- Client-Geräte können Anfragen an KSN initiieren, Informationen von KSN beziehen und Informationen an KSN übertragen, selbst wenn sie über keinen direkten Internetzugang verfügen.

- Die verarbeiteten Daten werden vom KSN-Proxyserver zwischengespeichert, wodurch die Belastung für den ausgehenden Datenverkehr verringert und das Empfangen der abgefragten Informationen durch das Client-Gerät beschleunigt wird.

Die Einstellungen des KSN-Proxyservers können Sie im Abschnitt **KSN-Proxy** im Eigenschaftenfenster des Administrationsservers ändern.

Zugriff auf KSN einrichten

Sie können den Zugriff auf Kaspersky Security Network (KSN) auf dem Administrationsserver und auf einem Verteilungspunkt anpassen.

Um den Zugriff des Administrationsservers auf KSN einzurichten, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Proxy** aus.

3. Setzen Sie den Schalter auf **KSN-Proxy auf dem Administrationsserver aktivieren Aktiviert**.

   Wenn diese Option aktiviert ist, sendet der KSN-Proxyserver Daten an KSN, um die Effizienz der Komponenten von Kaspersky Security Center zu erhöhen und die Leistung der Kaspersky-Anwendungen zu verbessern. Die Übertragung von Daten der Client-Geräte an KSN wird durch die Richtlinie von Kaspersky Endpoint Security vorgegeben, die auf den Client-Geräten angewendet wird. Wenn das Kontrollkästchen deaktiviert ist, werden vom Administrationsserver und von den Client-Geräten mittels Kaspersky Security Center Linux keine Daten an KSN übertragen. In diesem Fall können die Client-Geräte Daten entsprechend ihrer Einstellungen direkt an KSN übertragen (nicht über Kaspersky Security Center Linux). Die auf den Client-Geräten geltende Richtlinie für Kaspersky Endpoint Security bestimmt, welche Daten diese Geräte direkt (nicht über Kaspersky Security Center Linux) an KSN senden.

4. Wählen Sie die KSN-Infrastrukturlösung.

   Führen Sie im Unterabschnitt **Teilnahme an KSN** einen der folgenden Schritte aus:

   - Wenn Sie Global KSN verwenden, setzen Sie den Schalter auf **Kaspersky Security Network verwenden Aktiviert**.

     Wenn Sie diese Option aktivieren, müssen Sie die Bestimmungen der KSN-Erklärung lesen und akzeptieren.

   - Wenn Sie KPSN verwenden, stellen Sie den Umschalter auf die Position **Kaspersky Private Security Network verwenden Aktiviert** und klicken Sie auf die Schaltfläche **Datei mit KSN-Proxy-Einstellungen wählen**, um die Einstellungen für KPSN herunterzuladen (Dateien mit den Erweiterungen pkcs7 und pem). Nach dem Herunterladen der Einstellungen werden in der Benutzeroberfläche die Bezeichnung des Providers, die Kontaktdaten des Providers und das Erstellungsdatum der Datei mit Einstellungen von KPSN angezeigt.

   Wenn Sie den Umschalter in die Position **Kaspersky Private Security Network verwenden Aktiviert** stellen, erscheint eine Nachricht mit Details zu KPSN.

   Die folgenden Kaspersky-Anwendungen unterstützten KPSN:

   - Kaspersky Security Center Linux
   - Kaspersky Endpoint Security für Linux
   - Kaspersky Endpoint Security für Windows

   Wenn Sie KPSN in Kaspersky Security Center Linux aktivieren, erhalten diese Programme Informationen zur Unterstützung von KPSN. Im Unterabschnitt **Kaspersky Security Network** des Abschnitts **Erweiterter Schutz** wird im Fenster "Einstellungen" die Information zum ausgewählten KSN-Anbieter angezeigt: Entweder KSN oder KPSN.

Kaspersky Security Center Linux sendet keine statistischen Daten an Kaspersky Security Network, wenn im Eigenschaftenfenster des Administrationsservers im Abschnitt **KSN-Proxy** die Option "KPSN" konfiguriert ist.

5. Wenn Sie die Proxyserver-Einstellungen in den Eigenschaften des Administrationsservers angepasst haben, aber Ihre Netzwerkarchitektur eine direkte Verwendung von KPSN erfordert, aktivieren Sie die Option **Proxyserver-Einstellungen beim Verbinden mit KPSN ignorieren**. Andernfalls können Anfragen von den verwalteten Apps KPSN nicht erreichen.

6. Passen Sie die Einstellungen für die Verbindung des Administrationsservers mit dem Dienst des KSN-Proxy-Service an:

   - Geben Sie unter **Verbindungseinstellungen** für den **TCP-Port** die Nummer des TCP-Ports an, über den die Verbindung zum KSN-Proxyserver aufgebaut werden soll. Standardmäßig erfolgt die Verbindung zum KSN-Proxyserver über Port 13111.

   - Wenn Sie möchten, dass der Administrationsserver die Verbindung zum KSN-Proxyserver über einen UDP-Port herstellt, aktivieren Sie die Option **UDP-Port verwenden** und geben Sie eine Portnummer für den **UDP-Port** an. Standardmäßig ist diese Option deaktiviert und der TCP-Port wird verwendet. Wenn diese Option aktiviert wird, ist 15111 der standardmäßige UDP-Port für die Verbindung mit dem KSN-Proxyserver.

   - Wenn die verwalteten Geräte eine Verbindung mit dem Administrationsserver über einen HTTPS-Port herstellen sollen, aktivieren Sie die Option **HTTPS verwenden** und geben Sie anschließend im Feld **HTTPS-Port** eine Portnummer an. Standardmäßig ist diese Option deaktiviert und der TCP-Port wird verwendet. Wenn diese Option aktiviert wird, ist 17111 der standardmäßige HTTPS-Port für die Verbindung mit dem KSN-Proxyserver.

7. Stellen Sie den Umschalter auf die Position **Sekundäre Administrationsserver über den primären Administrationsserver mit KSN verbinden Aktiviert**.

   Wenn diese Option aktiviert ist, verwenden die sekundären Administrationsserver den primären Administrationsserver als KSN-Proxyserver. Wenn diese Option deaktiviert ist, verbinden sich die sekundären Administrationsserver selbständig mit KSN. In diesem Fall verwenden die verwalteten Geräte die sekundären Administrationsserver als KSN-Proxyserver.

   Die sekundären Administrationsserver verwenden den primären Administrationsserver als Proxyserver, wenn in den Eigenschaften der sekundären Administrationsserver im rechten Bereich des Abschnitts **KSN-Proxy** der Umschalter auf die Position **KSN-Proxy auf dem Administrationsserver aktivieren Aktiviert** gestellt ist.

8. Klicken Sie auf die Schaltfläche **Speichern**.

Daraufhin werden die Einstellungen für den Zugriff auf KSN gespeichert.

Sie können außerdem den Zugriff des Verteilungspunkts auf KSN anpassen, um z. B. die Auslastung des Administrationsservers zu reduzieren. Der Verteilungspunkt, der als KSN-Proxyserver fungiert, sendet KSN-Anfragen von verwalteten Geräten direkt an Kaspersky, ohne den Administrationsserver zu verwenden.

Um den Zugriff des Verteilungspunkts auf Kaspersky Security Network (KSN) einzurichten, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass der Verteilungspunkt manuell zugewiesen wurde.

2. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

3. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.
4. Klicken Sie auf den Namen des Verteilungspunkts, um das Fenster mit den Aufgabeneigenschaften zu öffnen.
5. Aktivieren Sie im Eigenschaftenfenster des Verteilungspunkts, im Abschnitt **KSN-Proxy** die Option **KSN-Proxy auf dem Verteilungspunkt aktivieren** und aktivieren Sie anschließend die Option **Direkt über das Internet auf KSN Cloud/KPSN zugreifen**.
6. Klicken Sie auf die Schaltfläche **OK**.

Der Verteilungspunkt wird nun als KSN-Proxyserver fungieren.

Beachten Sie, dass der Verteilungspunkt die Authentifizierung verwalteter Geräte mithilfe des NTLM-Protokolls nicht unterstützt.

Verwendung von KSN aktivieren und deaktivieren

So aktivieren Sie die Verwendung von KSN:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Proxy** aus.
3. Setzen Sie den Schalter auf **KSN-Proxy auf dem Administrationsserver aktivieren Aktiviert**.

Der KSN-Proxyserver ist aktiviert und sendet Daten an KSN, um die Effizienz der Komponenten von Kaspersky Security Center zu erhöhen und die Leistung der Kaspersky-Anwendungen zu verbessern.

1. Aktivieren Sie je nach der von Ihnen verwendeten Infrastruktur-Lösung für KSN die entsprechenden Schalter.
   - Wenn Sie Global KSN verwenden, setzen Sie den Schalter auf **Kaspersky Security Network verwenden Aktiviert**.

     Das Senden von Daten an KSN ist jetzt verfügbar. Wenn Sie diese Option aktivieren, müssen Sie die Bestimmungen der KSN-Erklärung lesen und akzeptieren.
   - Wenn Sie KPSN verwenden, setzen Sie den Schalter auf **Kaspersky Private Security Network verwenden Aktiviert** und klicken Sie anschließend auf die Schaltfläche **Datei mit KSN-Proxy-Einstellungen wählen**, um die Einstellungen für KPSN herunterzuladen (Dateien mit den Erweiterungen pkcs7 und pem). Nach dem Herunterladen der Einstellungen werden in der Benutzeroberfläche die Bezeichnung des Providers, die Kontaktdaten des Providers und das Erstellungsdatum der Datei mit KPSN-Einstellungen angezeigt.

     Wenn Sie den Schalter auf **Kaspersky Private Security Network verwenden Aktiviert** setzen, erscheint eine Nachricht mit Details zu KPSN.
2. Klicken Sie auf **Speichern**.

So deaktivieren Sie die Verwendung von KSN:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Proxy** aus.

3. Setzen Sie den Schalter auf **KSN-Proxy auf dem Administrationsserver aktivieren Deaktiviert**, um den KSN-Proxy-Dienst zu deaktivieren.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Die akzeptierte KSN-Erklärung anzeigen

Wenn Sie Kaspersky Security Network (KSN) aktivieren, müssen Sie die KSN-Erklärung lesen und akzeptieren. Sie können die akzeptierte KSN-Erklärung jederzeit anzeigen.

So zeigen Sie die akzeptierte KSN-Erklärung an:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Proxy** aus.

3. Klicken Sie auf den Link **Erklärung zu Kaspersky Security Network anzeigen**.

Im folgenden Fenster können Sie den Text der akzeptierten KSN-Erklärung anzeigen.

Eine aktualisierte KSN-Erklärung akzeptieren

Sie verwenden KSN gemäß der KSN-Erklärung, die Sie lesen und akzeptieren, wenn Sie KSN aktivieren. Wird die KSN-Erklärung aktualisiert, so wird sie Ihnen bei einem Upgrade der Version des Administrationsservers angezeigt. Sie können die aktualisierte KSN-Erklärung akzeptieren oder ablehnen. Wenn Sie diese ablehnen, verwenden Sie KSN weiterhin gemäß der Version der KSN-Erklärung, die Sie zuvor akzeptiert haben.

Nach dem Upgrade einer Version des Administrationsservers wird die aktualisierte KSN-Erklärung automatisch angezeigt. Wenn Sie die aktualisierte KSN-Erklärung ablehnen, können Sie diese später erneut anzeigen und akzeptieren.

So zeigen Sie die KSN-Erklärung an und akzeptieren sie anschließend:

1. Klicken Sie auf den Link **Benachrichtigungen anzeigen** in der oberen rechten Ecke des Programmhauptfensters.

   Das Fenster **Benachrichtigungen** wird geöffnet.

2. Klicken Sie auf den Link **Aktualisierte KSN-Erklärung anzeigen**.

   Das Fenster **Update der Erklärung zu Kaspersky Security Network** wird geöffnet.

3. Lesen Sie die KSN-Erklärung und klicken Sie je nach Ihrer Entscheidung auf eine der folgenden Schaltflächen:

   - **Ich akzeptiere die aktualisierte KSN-Erklärung**
   - **Ich verwende KSN unter der alten Erklärung**

   Entsprechend Ihrer Entscheidung funktioniert KSN in Übereinstimmung mit den Bedingungen der aktuellen oder der aktualisierten KSN-Erklärung. Das Anzeigen des Textes der akzeptierten KSN-Erklärung ist jederzeit in den Eigenschaften des Administrationsservers möglich.

Feststellen, ob der Verteilungspunkt als KSN-Proxyserver fungiert

Sie können auf einem verwalteten Gerät, welches als Verteilungspunkt fungiert, den Kaspersky Security Network-Proxy (KSN-Proxy) aktiveren. Ein verwaltetes Gerät funktioniert als KSN-Proxyserver, wenn auf dem Gerät der Dienst "ksnproxy" ausgeführt wird. Sie können diesen Dienst lokal auf dem Gerät überprüfen, aktivieren und deaktivieren.

Sie können einem Windows-basierten oder Linux-basierten Gerät die Rolle des Verteilungspunkts zuweisen. Die Methode zur der Überprüfung des Verteilungspunkts hängt vom Betriebssystem dieses Verteilungspunkts ab.

So stellen Sie fest, ob der Linux-basierte Verteilungspunkt als KSN-Proxyserver fungiert:

1. Führen Sie auf dem Gerät mit dem Verteilungspunkt den Befehl `ps aux` aus, um die Liste der ausgeführten Prozesse anzuzeigen.
2. Überprüfen Sie, ob in der Liste der laufenden Prozesse, der Prozess `/opt/kaspersky/klnagent64/sbin/ksnproxy` ausgeführt wird.

Wenn der Dienst `/opt/kaspersky/klnagent64/sbin/ksnproxy` ausgeführt wird, nimmt der Administrationsagent auf diesem Gerät an Kaspersky Security Network teil und fungiert als KSN-Proxyserver für verwaltete Geräte, die sich im Bereich des Verteilungspunkts befinden.

So stellen Sie fest, ob der Windows-basierte Verteilungspunkt als KSN-Proxyserver fungiert:

1. Öffnen Sie auf dem Gerät mit dem Verteilungspunkt unter Windows die **Dienste**-App (**Alle Programme** → **Windows Verwaltungsprogramme** → **Dienste**).
2. Prüfen Sie in der Liste der Dienste, ob der Dienst ksnproxy ausgeführt wird.

   Wenn der Dienst "ksnproxy" ausgeführt wird, nimmt der Administrationsagent auf diesem Gerät an Kaspersky Security Network teil und fungiert als KSN-Proxyserver für verwaltete Geräte, die sich im Bereich des Verteilungspunkts befinden.

Bei Bedarf können Sie den Dienst ksnproxy deaktivieren. In diesem Fall nimmt der Administrationsagent des Verteilungspunkts nicht länger an Kaspersky Security Network teil. Dieser Vorgang erfordert lokale Administratorrechte.

Statistiken des KSN-Proxyservers anzeigen

In der Kaspersky Security Center Web Console können Sie die Nutzungsstatistiken des KSN-Proxyservers anzeigen.

Die Statistik umfasst die folgenden Parameter:

- Verbindungsstatus mit KSN
- Anzahl der Cache-Einträge
- Anzahl der im Cache verarbeiteten Pakete
- Anzahl der empfangenen Pakete

Wenn Sie KPSN als Infrastruktur-Lösung verwenden, werden die Nutzungsstatistiken von KPSN angezeigt.

So zeigen Sie die Statistiken an:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Proxy** und öffnen Sie anschließend die Registerkarte **Statistik**.

   In diesem Abschnitt werden die aktuellen Nutzungsstatistiken des KSN-Proxyservers angezeigt. Die Statistiken werden alle 15 Sekunden aktualisiert.

Sie können Statistiken kopieren, indem Sie auf die Schaltfläche **In die Zwischenablage kopieren** klicken.

Aufgaben verwalten

In diesem Abschnitt werden Aufgaben beschrieben, die von Kaspersky Security Center Linux verwendet werden.

Über Aufgaben

Kaspersky Security Center Linux verwaltet die auf Geräten installierten Sicherheitsanwendungen von Kaspersky durch das Erstellen und Starten von *Aufgaben*. Die Aufgaben ermöglichen Installation, Start und Beenden von Anwendungen, Untersuchung von Dateien, Datenbanken-Update und Aktualisierung der Anwendungsmodule sowie Ausführung anderer Aktionen mit den Anwendungen.

Aufgaben für eine bestimmte Anwendung können mithilfe von Kaspersky Security Center Web Console nur dann erstellt werden, wenn das Verwaltungs-Plug-in für diese Anwendung auf dem Server der Web Console von Kaspersky Security Center installiert ist.

Aufgaben können auf dem Administrationsserver und auf Geräten ausgeführt werden.

Zu den Aufgaben, die auf dem Administrationsserver ausgeführt werden, gehören:

- Berichte automatisch versenden
- Updates in die Datenverwaltung herunterladen

- Backup der Daten des Administrationsservers anlegen
- Datenbank bedienen

Die folgenden Typen von Aufgaben werden auf Geräten ausgeführt:

- *Lokale Aufgaben* sind Aufgaben, die auf einem bestimmten Gerät ausgeführt werden.

  Lokale Aufgaben können entweder vom Administrator über Kaspersky Security Center Web Console geändert werden oder vom Benutzer eines Remote-Gerätes (beispielsweise über die Benutzeroberfläche einer Sicherheitsanwendungen). Wenn eine lokale Aufgabe gleichzeitig sowohl vom Administrator als auch vom Benutzer auf dem verwalteten Gerät geändert wurde, treten jene Änderungen in Kraft, die vom Administrator mit höherer Priorität ausgeführt wurden.

- *Gruppenaufgaben* sind Aufgaben, die auf allen Geräten einer bestimmten Gruppe ausgeführt werden.

  Soweit in den Aufgabeneigenschaften nicht anders festgelegt, betrifft eine Gruppenaufgabe auch alle Untergruppen der ausgewählten Gruppe. Eine Gruppenaufgabe betrifft (optional) auch Geräte, die mit den sekundären und virtuellen Administrationsservern in der Gruppe und den Untergruppen verbunden sind.

- *Globale Aufgaben* sind Aufgaben, die auf einem Satz von Geräten ausgeführt werden, und zwar unabhängig davon, ob sie zu einer Gruppe gehören.

Sie können für jede Anwendung eine beliebige Anzahl von Gruppenaufgaben, globalen Aufgaben oder lokalen Aufgaben erstellen.

Sie können die Aufgabeneinstellungen ändern, den Fortschritt von Aufgaben verfolgen, und Aufgaben kopieren, exportieren, importieren und löschen.

Eine Aufgabe wird auf einem Gerät nur dann gestartet, wenn die Anwendung gestartet wurde, für die diese Aufgabe erstellt wurde.

Ausführungsergebnisse von Aufgaben werden im Betriebssystem-Ereignisprotokolle auf jedem Gerät, im Betriebssystem-Ereignisprotokoll des Administrationsservers und in der Administrationsserver-Datenbank gespeichert.

Geben Sie in den Einstellungen der Aufgaben keine vertraulichen Daten an. Dazu gehört z. B. das Kennwort des Domänenadministrators.

Über den Gültigkeitsbereich von Aufgaben

Der *Gültigkeitsbereich einer Aufgabe* ist die Menge von Geräten, auf denen die Aufgabe ausgeführt wird. Es gibt folgende Arten von Gültigkeitsbereichen:

- Für eine *lokale Aufgabe* ist der Gültigkeitsbereich das Gerät selbst.
- Für eine *Aufgabe des Administrationsservers* ist der Gültigkeitsbereich der Administrationsserver.
- Für eine *Gruppenaufgabe* ist der Gültigkeitsbereich die Liste der Geräte, die in der Gruppe enthalten sind.

Beim Erstellen einer *globalen Aufgabe* können Sie die folgenden Methoden verwenden, um ihren Gültigkeitsbereich festzulegen:

- Bestimmte Geräte manuell festlegen.

  Als Adresse des Gerätes können Sie eine IP-Adresse (oder einen IP-Bereich) oder einen DNS-Namen verwenden. Sie können auch Netzwerkgeräte auswählen, die vom Administrationsserver erkannt wurden.

- Geräteliste aus einer txt-Datei mit den hinzuzufügenden Geräteadressen importieren (jede Adresse muss in einer eigenen Zeile stehen).

  Wenn Sie eine Geräteliste aus einer Datei importieren oder eine Liste manuell erstellen, und wenn die Geräte namentlich identifiziert werden, darf die Liste nur Geräte enthalten, deren Daten bereits in die Administrationsserver-Datenbank eingegeben wurden. Darüber hinaus müssen die Informationen entweder während einer bestehenden Verbindung der Geräte oder während einer Gerätesuche eingegeben worden sein.

- Geräteauswahl angeben.

  Im Laufe der Zeit ändert sich der Gültigkeitsbereich der Aufgabe, je nachdem, wie sich die Anzahl der Geräte ändert, die zur Auswahl gehören. Die Geräteauswahl kann aufgrund der Geräte-Attribute, einschließlich aufgrund der auf dem Gerät installierten Software, und aufgrund der dem Gerät zugewiesenen Tags strukturiert sein. Die Geräteauswahl ist die flexibelste Art zum Festlegen des Gültigkeitsbereichs einer Aufgabe.

  Aufgaben für die Geräteauswahlen werden immer nach Zeitplan durch den Administrationsserver ausgeführt. Solche Aufgaben werden auf Geräten, die keine Verbindung mit dem Administrationsserver haben, nicht ausgeführt. Aufgaben, deren Gültigkeitsbereich mithilfe anderer Methoden festgelegt ist, werden direkt auf Geräten ausgeführt und sind daher nicht von der Geräteverbindung zum Administrationsserver abhängig.

  Aufgaben für Geräteauswahlen werden nicht nach der lokalen Uhrzeit des Geräts, sondern nach der lokalen Uhrzeit des Administrationsservers ausgeführt. Aufgaben, deren Gültigkeitsbereich mithilfe anderer Methoden festgelegt ist, werden nach der lokalen Uhrzeit eines Geräts ausgeführt.

Aufgaben erstellen

So erstellen Sie eine Aufgabe:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.

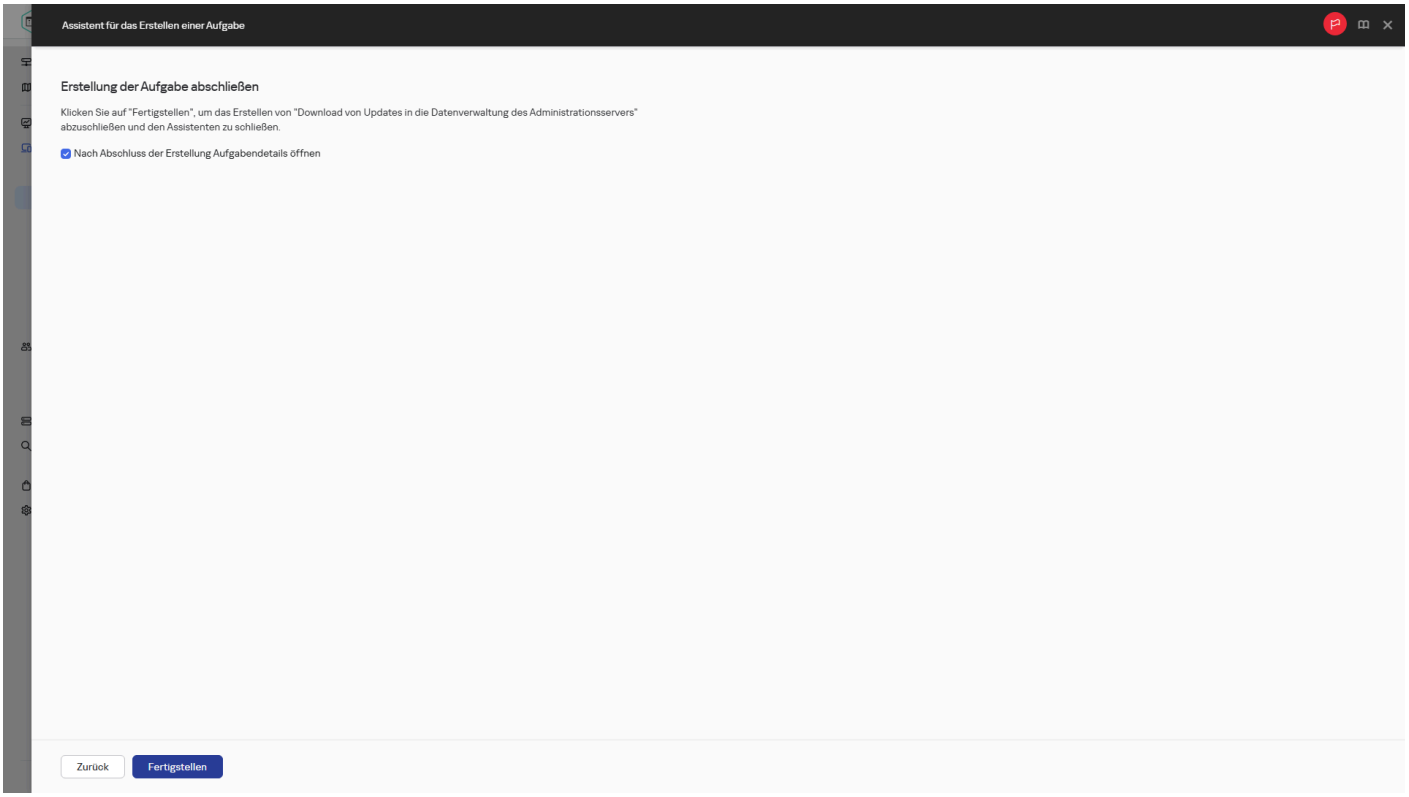
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie seinen Anweisungen.

3. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

4. Klicken Sie auf die Schaltfläche **Fertigstellen**.

Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.



Abschluss der Aufgabenerstellung

So erstellen Sie eine neue Aufgabe, die ausgewählten Geräten zugewiesen wird:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte)**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Aktivieren Sie in der Liste der verwalteten Geräte die Kontrollkästchen neben den Geräten, auf denen die Aufgabe ausgeführt werden soll. Sie können die Such- und Filterfunktionen verwenden, um die gewünschten Geräte zu finden.

3. Klicken Sie auf die Schaltfläche **Aufgabe starten** und wählen Sie anschließend **Neue Aufgabe hinzufügen** aus.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.

   Im ersten Schritt des Assistenten können Sie die ausgewählten Geräte entfernen, die für den Gültigkeitsbereich der Aufgabe ausgewählt waren. Folgen Sie den Anweisungen des Assistenten.

4. Klicken Sie auf die Schaltfläche **Fertigstellen**.

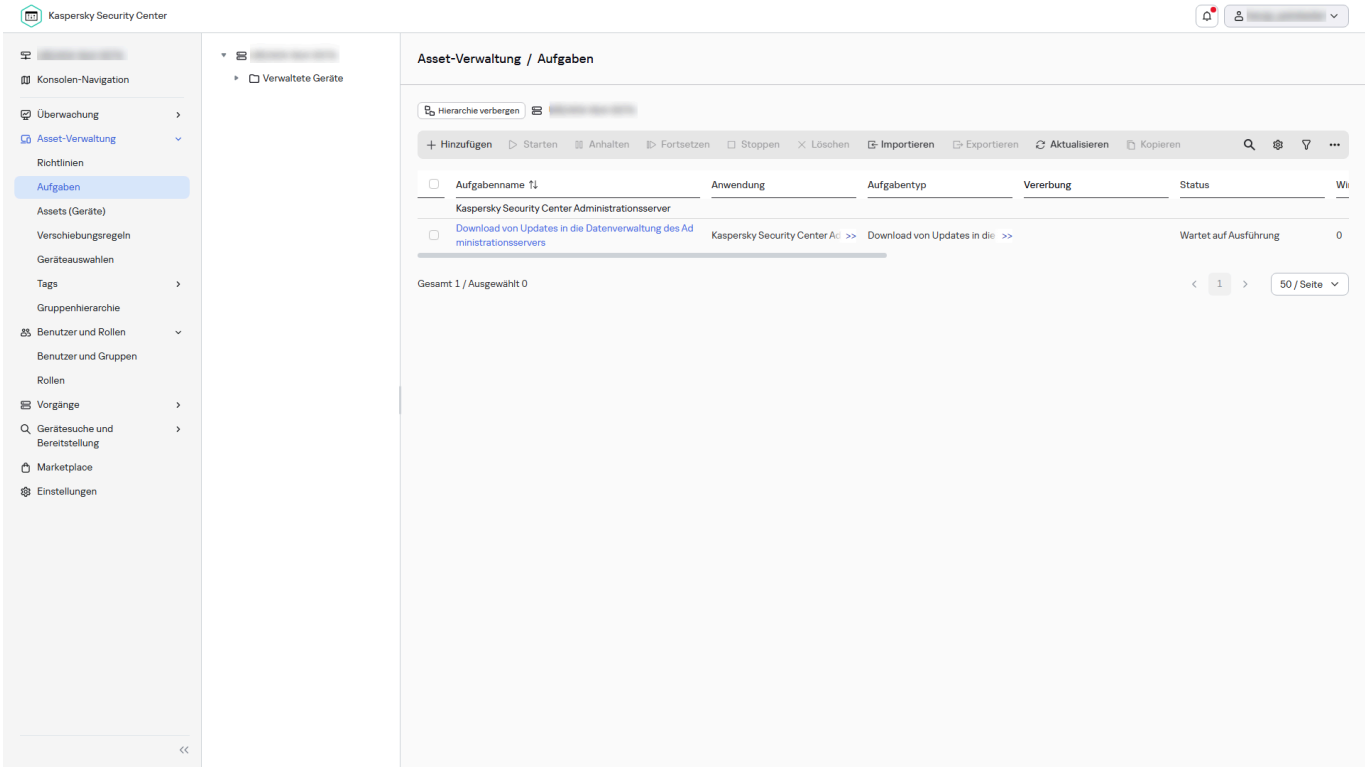
Die Aufgabe wird für die ausgewählten Geräte erstellt.

Aufgaben manuell starten

Die Anwendung startet Aufgaben gemäß den Zeitplaneinstellungen, die in den Eigenschaften der einzelnen Aufgaben angegeben sind. Sie können die Aufgabe jederzeit manuell aus der Aufgabenliste starten. Alternativ können Sie in der Liste **Assets (Geräte)** die gewünschten Geräte auswählen und anschließend eine vorhandene Aufgabe für diese starten.

So starten Sie eine Aufgabe manuell:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Aktivieren Sie in der Aufgabenliste das Kontrollkästchen neben der Aufgabe, die Sie starten möchten.
3. Klicken Sie auf die Schaltfläche **Starten**.



Starten einer Aufgabe aus der Aufgabenliste

Die Aufgabe wird gestartet. Sie können den Status der Aufgabe in der Spalte **Status** oder durch Anklicken der Schaltfläche **Ergebnis** überprüfen.

Eine Aufgabe für ausgewählte Geräte starten

Sie können mehrere Client-Geräte aus der Geräteliste auswählen und anschließend eine zuvor für diese erstellte Aufgabe starten. Auf diese Weise können Sie Aufgaben ausführen, die zuvor für eine bestimmte Geräteauswahl erstellt wurden.

Dadurch wird beim Starten der Aufgabe anstelle der Geräte, denen die Aufgabe ursprünglich zugewiesen war, die Liste mit den von Ihnen ausgewählten Geräten angewendet.

So starten Sie eine Aufgabe für ausgewählte Geräte:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**. Die Liste der verwalteten Geräte wird angezeigt.

2. Wählen Sie in der Liste der verwalteten Geräte mithilfe der Kontrollkästchen jene Geräte aus, für die Sie die Aufgabe ausführen möchten. Sie können die Such- und Filterfunktionen verwenden, um die gewünschten Geräte zu finden.

3. Klicken Sie auf die Schaltfläche **Aufgabe ausführen** und wählen Sie anschließend **Bestehende Aufgabe anwenden** aus.

   Die Liste der vorhandenen Aufgaben wird angezeigt.

4. Die ausgewählten Geräte werden oberhalb der Aufgabenliste angezeigt. Bei Bedarf können Sie Geräte aus dieser Liste entfernen. Die Liste muss mindestens ein Gerät enthalten.

5. Wählen Sie die gewünschte Aufgabe aus der Liste aus. Sie können das Suchfeld oberhalb der Liste verwenden, um die gewünschte Aufgabe anhand des Namens zu finden. Es kann nur eine Aufgabe ausgewählt werden.

6. Klicken Sie auf **Aufgabe speichern und ausführen**.

   Die ausgewählte Aufgabe wird sofort für die ausgewählten Geräte gestartet. Der konfigurierte Startzeitplan für den Aufgabenstart wird dabei nicht geändert.

Aufgabenliste anzeigen

Sie können die Liste der Aufgaben anzeigen, die in Kaspersky Security Center Linux erstellt wurden.

Um die Liste der Aufgaben anzuzeigen:

Wechseln Sie im Hauptmenü zu **Aufgaben**.

Die Aufgabenliste wird angezeigt. Die Aufgaben sind nach den Namen der Anwendungen gruppiert, auf die sie sich beziehen. Beispielsweise bezieht sich die Aufgabe *Remote-Installation einer Anwendung* auf den Administrationsserver, und die Aufgabe *Update* bezieht sich auf Kaspersky Endpoint Security.

Um die Eigenschaften einer Aufgabe anzuzeigen,

Klicken Sie auf den Namen der Aufgabe.

Das Fenster mit den Aufgabeneigenschaften enthält mehrere benannte Registerkarten. Zum Beispiel wird der **Aufgabentyp** auf der Registerkarte **Allgemein** angezeigt und der Aufgabenzeitplan auf der Registerkarte **Zeitplan**.

Allgemeine Aufgabeneinstellungen

Dieser Abschnitt enthält die Einstellungen, die Sie für Aufgaben anzeigen und konfigurieren können. Die Liste der verfügbaren Einstellungen hängt von der Aufgabe ab, die Sie konfigurieren.

Einstellungen, die während der Aufgabenerstellung festgelegt werden

Sie können beim Erstellen einer Aufgabe die folgenden Einstellungen festlegen. Einige dieser Einstellungen können auch in den Eigenschaften der erstellten Aufgabe geändert werden.

- Neustart-Einstellungen des Betriebssystems:
  - **Gerät nicht neu starten**

    Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

  - **Gerät neu starten**

    Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

  - **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

    Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

    Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

    Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

    Diese Option ist standardmäßig deaktiviert.

- Zeitplaneinstellungen für Aufgaben:

  Die Arten des Zeitplans können je nach Aufgabe variieren.

  Es ist möglich, dass einige Arten von Zeitplänen in anderen Kaspersky-Anwendungen nicht verfügbar sind.

  - **Einstellung Aufgabe starten:**
    - **Alle n Stunden**

      Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

      Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

- **Alle n Tage**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

  Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

- **Alle n Minuten**

  Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

  Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Manuell**

  Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

  Diese Variante ist standardmäßig ausgewählt.

- **Einmal**

  Die Aufgabe wird einmal zum angegebenen Datum und zur angegebenen Uhrzeit ausgeführt (standardmäßig entspricht dies dem Tag, an dem die Aufgabe erstellt wurde).

- **Sofort**

  Die Aufgabe wird nach dem Speichern der Einstellungen umgehend ausgeführt.

- **Monatlich am ausgewählten Tag**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Nach dem Download neuer Updates in die Datenverwaltung**

  Die Aufgabe wird gestartet, nachdem Updates in die Datenverwaltung heruntergeladen wurden. Sie können diesen Zeitplan beispielsweise die *Update*-Aufgabe verwenden.

- **Nach Abschluss einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Automatische zufällige Verzögerung des Aufgabenstarts innerhalb eines Intervalls von**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

- Geräte, denen die Aufgabe zugewiesen wird:

  - **Geräte auswählen, die vom Administrationsserver erkannt wurden**

    Die Aufgabe wird einer Reihe von Geräten zugewiesen. In dieser Reihe von Geräten können Sie sowohl Geräte aus den Administrationsgruppen als auch nicht zugeordnete Geräte aufnehmen.

    Sie können diese Option beispielsweise für eine Aufgabe zur Installation des Administrationsagenten auf nicht zugeordneten Geräten verwenden.

  - **Geräteadressen manuell angeben oder aus Liste importieren**

    Sie können DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die Aufgabe zugewiesen werden soll.

    Diese Option können Sie beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

  - **Aufgabe an eine Geräteauswahl zuweisen**

    Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

    Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

  - **Aufgabe einer Administrationsgruppe zuweisen**

    Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

    Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

    Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der Gruppen unterliegen, für die sie gelten.

- Benutzerkonto-Einstellungen:

  - **Standardbenutzerkonto**

    Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

    Diese Variante ist standardmäßig ausgewählt.

  - **Benutzerkonto angeben**

    Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

  - **Benutzerkonto**

    Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

- **Kennwort**

  Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

Einstellungen, die nach der Aufgabenerstellung festgelegt werden

Sie können die folgenden Einstellungen erst festlegen, nachdem eine Aufgabe erstellt wurde.

- Einstellungen der Gruppenaufgabe:

  - **Auf Untergruppen verteilen**

    Diese Option ist nur in den Einstellungen der Gruppenaufgaben verfügbar.

    Wenn diese Option aktiviert ist, umfasst der Gültigkeitsbereich der Aufgabe die folgenden Objekte:

    - Die Administrationsgruppe, die Sie beim Erstellen der Aufgabe ausgewählt haben.
    - Die Administrationsgruppen, die der ausgewählten Administrationsgruppe entsprechend der Gruppenhierarchie auf beliebiger Ebene untergeordnet sind.

    Wenn diese Option deaktiviert ist, umfasst der Gültigkeitsbereich der Aufgabe nur die Administrationsgruppe, die Sie beim Erstellen der Aufgabe ausgewählt haben.

    Diese Option ist standardmäßig aktiviert.

  - **An sekundäre und virtuelle Administrationsserver verteilen**

    Wenn diese Option aktiviert ist, wird die Aufgabe, die auf dem primären Administrationsserver wirksam ist, auch auf den sekundären Administrationsservern (einschließlich virtuellen) angewendet. Wenn auf dem sekundären Administrationsserver bereits eine Aufgabe des gleichen Typs existiert, werden auf dem sekundären Administrationsserver beide Aufgaben angewendet – die bestehende und die vom primären Administrationsserver übernommene.

    Diese Option ist nur verfügbar, wenn die Option **Auf Untergruppen verteilen** aktiviert ist.

    Diese Option ist standardmäßig deaktiviert.

- Erweiterte Zeitplaneinstellungen:

  - **Vor dem Aufgabenstart die Geräte mittels Wake-On-LAN hochfahren**

    Das Betriebssystem auf dem Gerät startet zum angegebenen Zeitpunkt, bevor die Aufgabe gestartet wird. Standardmäßig beträgt die Zeitspanne fünf Minuten.

    Aktivieren Sie diese Option, wenn Sie möchten, dass die Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich ausgeführt wird, einschließlich jener Geräte, die ausgeschaltet sind, wenn die Aufgabe gestartet werden soll.

    Wenn das Gerät nach Abschluss der Aufgabe automatisch ausgeschaltet werden soll, aktivieren Sie die Option **Geräte nach Abschluss der Aufgabe herunterfahren**. Die Option befindet sich im selben Fenster.

    Diese Option ist standardmäßig deaktiviert.

  - **Geräte nach Abschluss der Aufgabe herunterfahren**

    Sie können diese Option beispielsweise für eine Aufgabe zur Installation von Updates aktivieren, die Updates für Client-Geräte jeden Freitag nach Geschäftsschluss installiert und diese Geräte dann über das Wochenende abschaltet.

Diese Option ist standardmäßig deaktiviert.

- **Aufgabe unterbrechen, wenn deren Ausführung länger dauert als**

  Nachdem die festlegte Zeitspanne abgelaufen ist, wird die Aufgabe automatisch angehalten, egal ob sie abgeschlossen ist oder nicht.

  Aktivieren Sie diese Option, wenn Sie Aufgaben, deren Ausführung zu lange dauert, unterbrechen (oder anhalten) möchten.

  Diese Option ist standardmäßig deaktiviert. Die Standardzeit für die Aufgabenausführung beträgt 120 Minuten.

- Benachrichtigungseinstellungen:

  - Block **Ereignisdaten speichern**:

    - **In der Administrationsserver-Datenbank speichern für (Tage)**

      Anwendungsereignisse, die sich auf die Ausführung der Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich beziehen, werden auf dem Administrationsserver während der festgelegten Anzahl an Tagen gespeichert. Wenn diese Zeitspanne abgelaufen ist, werden die Informationen vom Administrationsserver gelöscht.

      Diese Option ist standardmäßig aktiviert.

    - **Im System-Ereignisprotokoll des Geräts speichern**

      Anwendungsereignisse, die sich auf die Ausführung der Aufgabe beziehen, werden lokal im Syslog-Ereignisprotokoll jedes Client-Gerätes gespeichert.

      Diese Option ist standardmäßig deaktiviert.

    - **Im System-Ereignisprotokoll des Administrationsservers speichern**

      Anwendungsereignisse, die sich auf die Ausführung der Aufgabe auf allen Client-Geräten aus dem Aufgabenbereich beziehen, werden zentral im Syslog-Ereignisprotokoll des Betriebssystems des Administrationsservers gespeichert.

      Diese Option ist standardmäßig deaktiviert.

    - **Alle Ereignisse speichern**

      Wenn diese Option ausgewählt ist, werden alle Ereignisse, die sich auf die Aufgabe beziehen, in den Ereignisprotokollen gespeichert.

    - **Ereignisse in Bezug auf den Aufgabenfortschritt speichern**

      Wenn diese Option ausgewählt ist, werden nur Ereignisse, die sich auf die Aufgabenausführung beziehen, in den Ereignisprotokollen gespeichert.

    - **Nur die Ergebnisse der Aufgabenausführung speichern**

      Wenn diese Option ausgewählt ist, werden nur Ereignisse, die sich auf die Ergebnisse der Aufgabenausführung beziehen, in den Ereignisprotokollen gespeichert.

- **Den Administrator über Ergebnisse der Aufgabenausführung benachrichtigen**

  Sie können die Methoden auswählen, über die Administratoren Benachrichtigungen über Ergebnisse der Aufgabenausführung erhalten: per E-Mail, mit SMS und durch Start einer ausführbaren Datei. Um die Benachrichtigungen zu konfigurieren, klicken Sie auf den Link **Einstellungen**.

  Standardmäßig sind alle Methoden der Zustellung von Benachrichtigungen deaktiviert.

- **Nur über Fehler benachrichtigen**

  Wenn diese Option aktiviert ist, werden Administratoren nur dann benachrichtigt, wenn die Aufgabenausführung mit einem Fehler beendet wird.

  Wenn diese Option deaktiviert ist, werden Administratoren nach jeder Aufgabenausführung benachrichtigt.

  Diese Option ist standardmäßig aktiviert.

- Sicherheitseinstellungen.

- Einstellungen für den Gültigkeitsbereich der Aufgabe.

  Abhängig davon, wie der Gültigkeitsbereich der Aufgabe bestimmt wird, sind die folgenden Einstellungen verfügbar:

  - **Geräte**

    Wenn der Gültigkeitsbereich einer Aufgabe durch eine Administrationsgruppe bestimmt wird, können Sie diese Gruppe anzeigen. Hier sind keine Änderungen möglich. Sie können aber **Ausschlüsse vom Gültigkeitsbereich der Aufgabe** festlegen.

    Wenn der Gültigkeitsbereich einer Aufgabe durch eine Liste von Geräten bestimmt wird, können Sie diese Liste ändern, indem Sie Geräte hinzufügen und entfernen.

  - **Geräteauswahl**

    Sie können die Geräteauswahl ändern, für welche die Aufgabe übernommen wird.

  - **Ausschlüsse vom Gültigkeitsbereich der Aufgabe**

    Sie können Gruppen von Geräten festlegen, für welche die Aufgabe nicht angewendet wird. Gruppen, die ausgeschlossen werden sollen, können sich nur den Untergruppen der Administrationsgruppe befinden, für welche die Aufgabe übernommen wird.

- **Revisionsverlauf**.

Aufgaben exportieren

Mit Kaspersky Security Center Linux können Sie eine Aufgabe und deren Einstellungen in einer klt-Datei speichern. Sie können diese klt-Datei verwenden, um sowohl in Kaspersky Security Center Windows als auch in Kaspersky Security Center Linux die gespeicherte Aufgabe zu importieren.

Um eine Aufgabe zu exportieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Aktivieren Sie das Kontrollkästchen neben der Aufgabe, die Sie exportieren möchten.

   Sie können nicht mehrere Aufgaben gleichzeitig exportieren. Wenn Sie mehr als eine Aufgabe auswählen, wird die Schaltfläche **Exportieren** deaktiviert. Die Aufgaben des Administrationsservers sind für den Export ebenfalls nicht verfügbar.
3. Klicken Sie auf die Schaltfläche **Exportieren**.
4. Geben Sie im folgenden Fenster **Speichern unter** den Namen und den Pfad der Aufgabendatei an. Klicken Sie auf **Speichern**.

   Das Fenster **Speichern unter** wird nur angezeigt, wenn Sie Google Chrome, Microsoft Edge oder Opera verwenden. Wenn Sie einen anderen Browser verwenden, wird die Aufgabendatei automatisch im Ordner **Downloads** gespeichert.

Aufgaben importieren

Mit Kaspersky Security Center Linux können Sie eine Aufgabe aus einer klt-Datei importieren. Die klt-Datei enthält die exportierte Aufgabe und deren Einstellungen.

Damit die Aufgabe einer Kaspersky-Anwendung korrekt importiert wird, müssen Sie das entsprechende Verwaltungs-Plug-in installieren.

Um eine Aufgabe zu importieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Importieren**.
3. Klicken Sie auf die Schaltfläche **Durchsuchen**, um eine Aufgabendatei auszuwählen, die Sie importieren möchten.
4. Geben Sie im folgenden Fenster den Pfad zur klt-Aufgabendatei an und klicken Sie anschließend auf die Schaltfläche **Öffnen**. Beachten Sie, dass Sie nur eine Aufgabendatei auswählen können.

   Die Verarbeitung der Aufgabe beginnt.
5. Nachdem die Aufgabe erfolgreich verarbeitet wurde, wählen Sie die Geräte aus, denen Sie die Aufgabe zuweisen möchten. Wählen Sie dazu eine der folgenden Optionen aus:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

- **Geräteadressen manuell angeben oder aus Liste importieren**

  Sie können DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die Aufgabe zugewiesen werden soll.

  Diese Option können Sie beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

6. Wählen Sie den Gültigkeitsbereich der Aufgabe aus.

7. Klicken Sie auf die Schaltfläche **Abgeschlossen**, um den Import der Aufgabe abzuschließen.

Die Benachrichtigung mit dem Resultat des Imports wird angezeigt. Wenn die Aufgabe erfolgreich importiert wurde, können klicken Sie auf den Link **Details**, um die Eigenschaften der Aufgabe anzuzeigen.

Nach einem erfolgreichen Import wird die Aufgabe in der Liste der Aufgaben angezeigt. Die Einstellungen und der Zeitplan der Aufgabe werden ebenfalls importiert. Die Aufgabe wird gemäß ihrem Zeitplan gestartet.

Wenn die neu importierte Aufgabe einen identischen Namen wie eine bereits vorhandene Aufgabe hat, wird der Name der importierten Aufgabe um den Index **(<nächste Sequenznummer>)** erweitert, zum Beispiel: **(1)**, **(2)**.

Assistent zum Ändern der Aufgabenkennwörter starten

Für eine nicht lokale Aufgabe können Sie ein Benutzerkonto angeben, unter dem die Aufgabe ausgeführt werden soll. Sie können das Benutzerkonto bei der Aufgabenerstellung oder in den Eigenschaften einer vorhandenen Aufgabe angeben. Wenn das angegebene Benutzerkonto den Sicherheitsvorschriften des Unternehmens unterliegt, müssen Sie das Benutzerkonto-Kennwort möglicherweise von Zeit zu Zeit ändern. Wenn das Benutzerkonto-Kennwort abläuft und Sie ein neues festlegen, müssen Sie das neue gültige Kennwort in den Aufgabeneigenschaften angeben, damit die Aufgaben korrekt starten können.

Mit dem Assistenten zum Ändern der Aufgabenkennwörter können Sie das alte Kennwort in allen Aufgaben, in denen das Benutzerkonto angegeben ist, automatisch durch das neue Kennwort ersetzen. Alternativ können Sie das Kennwort auch manuell in den Eigenschaften der einzelnen Aufgaben ändern.

Um den Assistenten zum Ändern der Aufgabenkennwörter zu starten:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.

2. Klicken Sie auf die Schaltfläche **Benutzerkonto-Anmeldedaten für den Aufgabenstart verwalten**.

Folgen Sie den Anweisungen des Assistenten.

Schritt 1. Anmeldedaten angeben

Geben Sie neue Anmeldedaten an, die derzeit in Ihrem System gültig sind. Wenn Sie zum nächsten Schritt des Assistenten wechseln, überprüft Kaspersky Security Center Linux, ob der angegebene Benutzerkonto-Name mit dem Benutzerkonto-Namen in den Eigenschaften der einzelnen nicht lokalen Aufgaben übereinstimmt. Stimmen die Benutzerkonto-Namen überein, so wird das Kennwort in den Aufgabeneigenschaften automatisch durch das neue ersetzt.

Um das neue Konto anzugeben, wählen Sie eine Option aus:

- **Aktuelles Benutzerkonto verwenden**

  Der Assistent verwendet den Namen des Kontos, unter dem Sie derzeit bei Kaspersky Security Center Web Console angemeldet sind. Geben Sie dann manuell das Kontokennwort in dem Feld **Aktuelles Kennwort für die Verwendung in Aufgaben** ein.

- **Anderes Benutzerkonto angeben**

  Geben Sie den Namen des Kontos an, unter dem die Aufgaben gestartet werden sollen. Geben Sie dann das Kontokennwort in dem Feld **Aktuelles Kennwort für die Verwendung in Aufgaben** ein.

Wenn Sie das Feld **Vorheriges Kennwort (optional; wenn Sie es durch das Aktuelle ersetzen wollen)** ausfüllen, ersetzt Kaspersky Security Center Linux das Kennwort nur für jene Aufgaben, in denen sowohl der Benutzerkonto-Name als auch das alte Kennwort gefunden werden. Das Ersetzen erfolgt automatisch. In allen übrigen Fällen müssen Sie eine Aktion auswählen, die beim nächsten Schritt des Assistenten ausgeführt werden soll.

Schritt 2. Auszuführenden Vorgang auswählen

Wenn Sie beim ersten Schritt des Assistenten das alte Kennwort nicht angegeben haben oder das angegebene alte Kennwort nicht mit den Kennwörtern in den Aufgabeneigenschaften übereinstimmt, müssen Sie eine Aktion auswählen, die für die gefundenen Aufgaben ausgeführt werden soll.

So wählen Sie eine Aktion für eine Aufgabe aus:

1. Aktivieren Sie das Kontrollkästchen neben der Aufgabe, für die Sie eine Aktion wählen möchten.
2. Führen Sie eine der folgenden Optionen aus:

   - Um das Kennwort in den Aufgabeneigenschaften zu entfernen, klicken Sie auf **Anmeldedaten löschen**.

     Die Aufgabe wird so angepasst, dass sie unter dem Standardkonto ausgeführt wird.

   - Um das Kennwort durch das neue zu ersetzen, klicken Sie auf **Die Änderung des Kennworts erzwingen, selbst wenn das alte Kennwort falsch oder nicht angegeben ist**.

   - Um die Kennwortänderung abzubrechen, klicken Sie auf **Es ist keine Aktion ausgewählt**.

   Die ausgewählten Aktionen werden angewendet, wenn Sie zum nächsten Schritt des Assistenten gewechselt sind.

Schritt 3. Ergebnisse anzeigen

Zeigen Sie beim letzten Schritt des Assistenten die Ergebnisse die einzelnen gefundenen Aufgaben an. Klicken Sie auf **Fertig stellen**, um den Assistenten abzuschließen.

Auf dem Administrationsserver gespeicherte Ergebnisse der Aufgabenausführung anzeigen

Kaspersky Security Center Linux erlaubt Ihnen, die Ausführungsergebnisse für Gruppenaufgaben, Aufgaben für eine Reihe von Geräten und Aufgaben des Administrationsservers anzuzeigen.

Um sich die Ergebnisse der Aufgabenausführung anzeigen zu lassen, gehen Sie wie folgt vor:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Allgemein** aus.
2. Öffnen Sie mithilfe des Links **Ergebnisse** das Fenster **Ergebnisse der Aufgabenausführung**.

So zeigen sie die Ergebnisse der Aufgabenausführung für einen sekundären Administrationsserver an:

1. Wählen Sie im Eigenschaftenfenster der Aufgabe den Abschnitt **Allgemein** aus.
2. Öffnen Sie mithilfe des Links **Ergebnisse** das Fenster **Ergebnisse der Aufgabenausführung**.
3. Klicken Sie auf **Statistiken von sekundären Servern**.
4. Wählen Sie den sekundären Server aus, für den Sie das Fenster **Ergebnisse der Aufgabenausführung** anzeigen möchten.

Programm-Tags

Dieser Abschnitt erklärt die Tags für Anwendungen und bietet eine Anleitung für deren Erstellung und Änderung sowie für das Zuweisen von Tags an Drittanbieteranwendungen.

Programm-Tags

Mit Kaspersky Security Center Linux können Sie den Anwendungen in der Programm-Registry Tags hinzufügen. Ein Tag ist eine Bezeichnung, anhand derer Anwendungen gruppiert und gefunden werden können. Einer Anwendung zugewiesene Tags können als Bedingung in den Geräteauswahlen verwendet werden.

Sie können z. B. das Tag `[Browser]` erstellen und es Browsern wie Microsoft Internet Explorer, Google Chrome, Mozilla Firefox usw. zuweisen.

Programm-Tag erstellen

Um ein Anwendungs-Tag zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Anwendungs-Tags**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Ein neues Tag-Fenster öffnet sich.
3. Geben Sie den Tag-Namen ein.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Das neue Tag wird in der Liste der Anwendungs-Tags angezeigt.

Anwendungs-Tag umbenennen

Um ein Anwendungs-Tag umzubenennen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Anwendungs-Tags**.
2. Aktivieren Sie das Kontrollkästchen neben dem Tag, das Sie umbenennen möchten, und klicken Sie auf **Bearbeiten**.

   Ein Fenster mit den Tag-Eigenschaften wird geöffnet.
3. Ändern Sie den Tag-Namen.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu speichern.

Das aktualisierte Tag wird in der Liste der Anwendungs-Tags angezeigt.

Einem Programm Tags zuweisen

Um einer Anwendung ein oder mehrere Tags zuzuweisen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Programm-Registry**.
2. Klicken Sie auf den Namen der Anwendung, dem Sie Tags zuweisen möchten.
3. Wählen Sie die Registerkarte **Tags** aus.

   Die Registerkarte zeigt alle Anwendungs-Tags an, die auf dem Administrationsserver vorhanden sind. Das Kontrollkästchen in der Spalte **Tag zugewiesen** ist für alle Tags aktiviert, die der ausgewählten Anwendung zugewiesen sind.

4. Aktivieren Sie in der Spalte **Tag zugewiesen** die Kontrollkästchen der Tags, die Sie zuweisen möchten.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

   Die Tags werden der Anwendung zugewiesen.

Zugewiesene Tags von einem Programm entfernen

Um ein oder mehrere Tags von einer Anwendung zu entfernen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Programm-Registry**.
2. Klicken Sie auf den Namen der Anwendung, von dem Sie Tags entfernen möchten.
3. Wählen Sie die Registerkarte **Tags** aus.

   Die Registerkarte zeigt alle Anwendungs-Tags an, die auf dem Administrationsserver vorhanden sind. Das Kontrollkästchen in der Spalte **Tag zugewiesen** ist für alle Tags aktiviert, die dem ausgewählten Programm zugewiesen sind.
4. Deaktivieren Sie in der Spalte **Tag zugewiesen** die Kontrollkästchen der Tags, die Sie entfernen möchten.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Tags werden von der Anwendung entfernt.

> Die entfernten Tags werden nicht gelöscht. Bei Bedarf können Sie diese manuell löschen.

Programm-Tag löschen

Um ein Anwendungs-Tag zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Anwendungs-Tags**.
2. Wählen Sie in der Liste das Anwendungs-Tag aus, das Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **OK**.

Das Anwendungs-Tag wird gelöscht. Das gelöschte Tag wird automatisch von allen Anwendungen entfernt, denen es zugewiesen war.

Tool "klscflag" zum Öffnen des Ports 13291 verwenden

Sie können Kaspersky Security Center Linux mithilfe des Tools "klakaut" automatisieren. Das Tool "klakaut" und das entsprechende Hilfesystem befinden sich im Installationsordner von Kaspersky Security Center Linux. Wenn Sie das Tool "klakaut" verwenden möchten, öffnen Sie den Port 13291 mithilfe des Tools "klscflag".

Das Tool "klscflag" ändert den Wert des Parameters KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Um den Port 13291 zu öffnen:

1. Führen Sie den folgenden Befehl in der Befehlszeile aus:
   ```
   /opt/kaspersky/ksc64/sbin/klscflag -ssvset -pv klserver -s 87 -n
   KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv true -svt BOOL_T -ss "|ss_type =
   \"SS_SETTINGS\";"
   ```

2. Starten Sie den Dienst des Kaspersky Security Center Administrationsservers neu, indem Sie den folgenden Befehl ausführen:
   ```
   sudo systemctl restart kladminserver_srv
   ```

   Der Port 13291 ist geöffnet.

Um zu überprüfen, ob Port 13291 erfolgreich geöffnet wurde:

Führen Sie den folgenden Befehl in der Befehlszeile aus:

```
/opt/kaspersky/ksc64/sbin/klscflag -ssvget -pv klserver -s 87 -n
KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

Dieser Befehl gibt das folgende Ergebnis zurück:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

Der Wert `true` gibt an, dass der Port geöffnet ist. Andernfalls wird der Wert `false` angezeigt.

Die Kaspersky Industrial CyberSecurity for Networks in der Kaspersky Security Center Web Console registrieren

Um mit der Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks über die Kaspersky Security Center Web Console zu arbeiten, müssen Sie die Web-Oberfläche zunächst in der Kaspersky Security Center Web Console registrieren.

So registrieren Sie die Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks:

1. Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind:

   - Sie haben das Web-Plug-in von Kaspersky Industrial CyberSecurity for Networks heruntergeladen und installiert.

     Sie können dies auch später tun, während Sie auf die Synchronisierung des Servers von Kaspersky Industrial CyberSecurity for Networks mit dem Administrationsserver warten. Nachdem das Plug-in heruntergeladen und installiert ist, wird der Abschnitt **KICS for Networks** im Hauptmenü der Kaspersky Security Center Web Console angezeigt.

   - In der Benutzeroberfläche von Kaspersky Industrial CyberSecurity for Networks ist die Interaktion mit Kaspersky Security Center konfiguriert und aktiviert. Weitere Informationen finden Sie in der Online-Hilfe von Kaspersky Industrial CyberSecurity for Networks.

2. Verschieben Sie das Gerät mit dem installierten Server von Kaspersky Industrial CyberSecurity for Networks von Gruppe "Nicht zugeordnete Geräte" in die Gruppe "Verwaltete Geräte":

   a. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung → Nicht zugewiesene Geräte**.

   b. Aktivieren Sie das Kontrollkästchen neben dem Gerät mit dem installierten Server von Kaspersky Industrial CyberSecurity for Networks.

   c. Klicken Sie auf die Schaltfläche **In Gruppe verschieben**.

   d. Aktivieren Sie in der Hierarchie der Administrationsgruppen das Kontrollkästchen neben der Gruppe **Verwaltete Geräte**.

   e. Klicken Sie auf die Schaltfläche **Verschieben**.

3. Öffnen Sie das Eigenschaftenfenster des Geräts mit dem installierten Server von Kaspersky Industrial CyberSecurity for Networks.

4. Wählen Sie in den Geräteeigenschaften im Abschnitt **General** die Option **Verbindung zum Administrationsserver nicht trennen** aus und klicken Sie anschließend auf **Speichern**.

5. Wählen Sie im Eigenschaftenfenster des Geräts den Abschnitt **Programme** aus.

6. Wählen Sie im Abschnitt **Programme** die Option "Kaspersky Security Center Administrationsagent" aus.

7. Wenn der aktuelle Status des Geräts auf *Angehalten* steht, warten Sie, bis dieser auf *Gestartet* wechselt.

   Dies kann bis zu 15 Minuten dauern. Wenn Sie das Web-Plug-in für Kaspersky Industrial CyberSecurity for Networks noch nicht installiert haben, können Sie dies jetzt tun.

8. Wenn Sie die Statistiken zu Kaspersky Industrial CyberSecurity for Networks anzeigen wollen, können Sie dem Dashboard entsprechende Widgets hinzufügen. So fügen Sie die Widgets hinzu:

   a. Gehen Sie im Hauptmenü zu **Überwachung → Dashboard**.

   b. Klicken Sie im Dashboard auf die Schaltfläche **Widget hinzufügen oder wiederherstellen**.

   c. Wählen Sie im geöffneten Widget-Menü die Option **Andere**.

d. Wählen Sie die Widgets aus, die Sie hinzufügen möchten.

- Bereitstellungs-Übersicht für KICS for Networks
- Informationen über die Server von KICS for Networks
- Aktuelle Ereignisse von KICS for Networks
- Geräte mit Vorfällen in KICS for Networks
- Kritische Ereignisse in KICS for Networks
- Statuswerte in KICS for Networks

9. Wechseln Sie wie folgt zur Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks:

a. Gehen Sie im Hauptmenü zu **KICS for Networks → Suchen**.

b. Klicken Sie auf die Schaltfläche **Ereignisse oder Geräte finden**.

c. Klicken Sie im angezeigten Fenster **Abfrage-Einstellungen** auf das Feld **Server**.

d. Wählen Sie in der Dropdown-Liste mit den Servern, die in Kaspersky Security Center integriert sind, den Punkt "Kaspersky Industrial CyberSecurity for Networks Server" aus und klicken Sie auf die Schaltfläche **Suchen**.

e. Klicken Sie auf den Link **Zum Server wechseln** neben dem Namen des Servers von Kaspersky Industrial CyberSecurity for Networks.

Es wird die Anmeldeseite von Kaspersky Industrial CyberSecurity for Networks angezeigt.

> Um sich an der Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks anzumelden, benötigen Sie ein Benutzerkonto für diese Anwendung.

Benutzer und Benutzerrollen verwalten

In diesem Abschnitt werden Benutzer und Benutzerrollen beschrieben und Anweisungen zum Erstellen und Ändern dieser Regeln, zum Zuweisen von Rollen und Gruppen zu Benutzern sowie zum Zuordnen von Richtlinienprofilen zu Rollen zur Verfügung gestellt.

Über Benutzerkonten

In Kaspersky Security Center Linux können Benutzerkonten und Sicherheitsgruppen verwaltet werden. Das Programm unterstützt drei Arten von Benutzerkonten:

- Benutzerkonten für Mitarbeiter einer Organisation. Der Administrationsserver erhält Daten über die Konten dieser Domänenbenutzer beim Abfragen des Domänencontrollers des Unternehmens.
- Benutzerkonten für lokale Benutzer. Lokale Benutzerkonten auf verwalteten Geräten sowie lokale Benutzerkonten auf dem Gerät mit dem installiertem Administrationsserver.
- Benutzerkonten für interne Benutzer von Kaspersky Security Center Linux. Sie können Konten von internen Benutzern erstellen. Diese Benutzerkonten werden nur innerhalb von Kaspersky Security Center Linux verwendet.

In Kaspersky Security Center Linux kann die Gruppe "kladmins" nicht für den Zugriff auf die Kaspersky Security Center Web Console verwendet werden. Die Gruppe "kladmins" kann nur Benutzerkonten enthalten, die zum Starten der Dienste von Kaspersky Security Center Linux verwendet werden.

So zeigen Sie Tabellen mit Benutzerkonten und Sicherheitsgruppen an:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen**.
2. Wählen Sie die Registerkarte **Benutzer** oder **Gruppen** aus.

Die Tabelle mit den Benutzern oder Sicherheitsgruppen wird geöffnet. Wenn Sie in der Tabelle nur interne Benutzer oder Gruppen, bzw. nur lokale Benutzern oder Gruppen anzeigen möchten, setzen Sie das Filterkriterium für **Typ des Kontos** auf **Intern** bzw. **Lokal**.

Wenn die Tabelle der Benutzer mehr als 50.000 Benutzer enthält, werden nur die ersten 50.000 Benutzer angezeigt und die restlichen Benutzer nicht.

Über Benutzerrollen

Eine *Benutzerrolle* (auch als *Rolle* bezeichnet) ist ein Objekt, das einen Satz von Rechten und Berechtigungen enthält. Eine Rolle kann mit Einstellungen von Anwendungen von Kaspersky verbunden sein, die auf einem Benutzergerät installiert sind. Sie können einem Satz von Benutzern oder einem Satz von Sicherheitsgruppen eine Rolle auf jeder Hierarchieebene von Administrationsgruppen, Administrationsservern oder auf Ebene spezieller Objekte zuweisen.

Wenn Sie Geräte über eine Hierarchie von Administrationsservern verwalten, die auch virtuelle Administrationsserver umfasst, beachten Sie, dass Sie Benutzerrollen nur auf dem primären Administrationsserver erstellen, ändern oder löschen können. Anschließend können Sie die Benutzerrollen an sekundäre Administrationsserver, einschließlich virtueller, weitergeben.

Sie können Benutzerrollen mit Richtlinienprofilen verbinden. Wenn einem Benutzer eine Rolle zugewiesen ist, erhält dieser Benutzer Sicherheitseinstellungen, die zur Durchführung der Aufgabenfunktionen erforderlich sind.

Eine Benutzerrolle kann mit Benutzern von Geräten in einer bestimmten Administrationsgruppe verbunden sein.

Benutzerrollenbereich

Ein *Benutzerrollenbereich* ist eine Kombination von Benutzern und Administrationsgruppen. Einstellungen, die mit einer Benutzerrolle verbunden sind, gelten nur für Geräte, die Benutzern gehören, die über diese Rolle verfügen, und nur, wenn diese Geräte zu Gruppen gehören, die mit dieser Rolle verbunden sind, einschließlich untergeordnete Gruppen.

Vorteil der Verwendung von Rollen

Ein Vorteil der Verwendung von Rollen ist, dass Sie Sicherheitseinstellungen nicht für jedes der verwalteten Geräte oder für jeden der Benutzer separat festlegen müssen. Die Anzahl von Benutzern und Geräten in einem Unternehmen kann recht groß sein, die Anzahl von unterschiedlichen Stellenfunktionen, für die unterschiedliche Sicherheitseinstellungen erforderlich sind, ist jedoch erheblich kleiner.

Unterschiede verglichen mit Verwendung von Richtlinienprofilen

Richtlinienprofile sind Eigenschaften einer Richtlinie, die für jede Kaspersky-Anwendung separat erstellt wird. Eine Rolle ist mit vielen Richtlinienprofilen verbunden, die für unterschiedliche Anwendungen erstellt wurden. Eine Rolle ist daher eine Methode zur Vereinigung von Einstellungen für einen bestimmten Benutzertyp an einem Ort.

Zugriffsrechte auf Programmfunktionen konfigurieren. Rollenbasierte Zugriffskontrolle

Kaspersky Security Center Linux unterstützt eine rollenbasierte Zugriffskontrolle auf die Funktionen von Kaspersky Security Center Linux und von verwalteten Kaspersky-Anwendungen.

Sie können die Zugriffsrechte auf Anwendungsfunktionen für Benutzer von Kaspersky Security Center Linux mit einer der folgenden Methoden konfigurieren:

- Durch individuelle Konfiguration der Berechtigungen jedes Benutzers bzw. jeder Benutzergruppe.
- Durch Erstellen typischer Benutzerrollen mit einer vordefinierten Auswahl von Berechtigungen und Zuweisung der Rollen an die Benutzer, wobei deren Verantwortungsbereiche berücksichtigt werden.

Die Verwendung von Benutzerrollen soll wiederkehrende Abläufe für das Konfigurieren von Zugriffsrechten der Benutzer auf Anwendungsfunktionen vereinfachen und verkürzen. Die Zugriffsberechtigungen werden in einer Rolle nach den typischen Aufgaben und Verantwortungsbereichen des Benutzers festgelegt.

Die Benutzerrollen können nach dem jeweiligen Verwendungszweck benannt werden. Sie können eine unbegrenzte Anzahl von Rollen in der Anwendung erstellen.

Sie können entweder vordefinierte Benutzerrollen mit bereits festgelegten Zugriffsrechten verwenden oder neue Rollen erstellen und die notwendigen Berechtigungen selbst konfigurieren.

Zugriffsrechte auf Programmfunktionen

Die folgende Tabelle zeigt die Funktionen von Kaspersky Security Center Linux mit den Zugriffsrechten zur Verwaltung der damit verknüpften Aufgaben, Berichte und Einstellungen sowie für die Durchführung der damit verknüpften Benutzervorgänge an.

Um einen in der Tabelle aufgeführten Vorgang auszuführen, muss der Benutzer die rechts neben dem Vorgang angegebene Berechtigung besitzen.

Die Berechtigungen **Lesen**, **Schreiben** und **Ausführen** können auf jede Aufgabe, jeden Bericht und jede Einstellung angewendet werden. Zusätzlich zu diesen Berechtigungen muss ein Benutzer über die Berechtigung **Vorgänge auf Geräteauswahl durchführen** verfügen, um Aufgaben, Berichte oder Einstellungen auf Geräteauswahlen zu verwalten.

> Alle Aufgaben, Berichte, Einstellungen und Installationspakete, die in der Tabelle fehlen, gehören zum Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen**.

Zugriffsrechte auf Programmfunktionen

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
Allgemeine Funktionen: **Verwaltung von Administrationsgruppen**	**Schreiben**	• Hinzufügen eines Geräts zu einer Administrationsgruppe: **Schreiben** • Löschen eines Geräts aus einer Administrationsgruppe: **Schreiben** • Hinzufügen einer Administrationsgruppe zu einer anderen Administrationsgruppe: **Schreiben** • Löschen einer Administrationsgruppe aus einer anderen Administrationsgruppe: **Schreiben**	Keine	Nichts

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
Allgemeine Funktionen: **Zugriff auf Objekte, unabhängig von ihren ACLs**	**Lesen**	Lesezugriff auf alle Objekte erhalten: **Lesen**	Nichts	Nichts

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
Allgemeine Funktionen: **Grundlegende Funktionen**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Regeln für das Verschieben von Geräten (erstellen, ändern, löschen) für den virtuellen Server: **Schreiben**, **Vorgänge auf Geräteauswahlen ausführen** • Benutzerdefiniertes Zertifikat des Mobilfunkprotokolls (LWNGT) erhalten: **Lesen** • Benutzerdefiniertes Zertifikat des Mobilfunkprotokolls (LWNGT) festlegen: **Schreiben** • NLA-definierte Netzwerkliste erhalten: **Lesen** • NLA-definierte Netzwerkliste hinzufügen, ändern oder löschen: **Schreiben** • Liste der Zugriffskontrolle von Gruppen anzeigen: **Lesen** • Anzeigen des Betriebssystem-Protokolls: **Lesen** • Anzeigen des Wiederherstellungsschlüssels, um den Zugriff auf eine mit BitLocker-Laufwerkverschlüsselung verschlüsselte Festplatte wiederherzustellen: **Ausführen**	• "Download von Updates in die Datenverwaltung des Administrationsservers" • "Berichte senden" • "Installationspaket verteilen" • "Remote-Installation einer Anwendung auf sekundären Administrationsservern"	• "Bericht über Schutzstatus • "Bericht über Bedrohungen • "Bericht über stärksten infi Geräte" • "Bericht über Status der A Datenbanken • "Fehlerberich • "Bericht über Netzwerkang • "Zusammenfa Bericht über Schutzprogr das E-Mail-S • "Zusammenfa Bericht über Anwendunge Schutz von Workstations Windows Ser • "Zusammenfa Bericht über Anwendunge Perimetersch • "Zusammenfa Bericht über Anwendungs • "Bericht über Benutzer infi Geräte" • "Bericht über Sicherheitsp • "Ereignisberic • "Bericht über Aktivität von Verteilungsp • "Bericht über sekundäre Administratic • "Bericht über Ereignisse de Gerätekontro • "Bericht über Schwachstel • "Bericht über verbotene Pr • "Bericht über Kontrolle" • "Bericht über Verschlüssel verwalteter C • "Bericht über Verschlüssel der Massenspeic • "Bericht über Zugriffsrecht verschlüsselt Laufwerke" • "Bericht über der Dateiverschli • "Bericht über Zugriffe auf verschlüsselt • "Bericht über Benutzerrech • "Bericht über Berechtigung
Allgemeine Funktionen:	• **Lesen**	• Gelöschte Objekte im	Nichts	Nichts

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
Gelöschte Objekte	• **Schreiben**	Papierkorb anzeigen: **Lesen** • Objekte aus dem Papierkorb löschen: **Schreiben**		
Allgemeine Funktionen: **Verarbeitung von Ereignissen**	• **Ereignisse löschen** • **Einstellungen der Ereignisbenachrichtigung bearbeiten** • **Einstellungen der Ereignisprotokollierung bearbeiten** • **Schreiben**	• Einstellungen der Ereignisregistrierung ändern: **Einstellungen der Ereignisprotokollierung bearbeiten** • Einstellungen der Ereignisbenachrichtigung ändern: **Einstellungen der Ereignisbenachrichtigung bearbeiten** • Ereignisse löschen: **Ereignisse löschen**	Nichts	Nichts
Allgemeine Funktionen: **Vorgänge auf dem Administrationsserver**	• **Lesen** • **Schreiben** • **Ausführen** • **Objekt-ACLs ändern** • **Vorgänge auf Geräteauswahlen ausführen**	• Ports des Administrationsservers für die Verbindung zum Administrationsagenten angeben: **Schreiben** • Ports des auf dem Administrationsserver gestarteten Aktivierungsproxy angeben: **Schreiben** • Ports des auf dem Administrationsserver gestarteten Aktivierungsproxy für mobile Geräte angeben: **Schreiben** • Ports des Webservers für die Verteilung von autonomen Paketen angeben: **Schreiben** • Ports des Webservers für die Verteilung von MDM-Profilen angeben: **Schreiben** • SSL-Ports des Administrationsservers für die Verbindung mittels Web Console angeben: **Schreiben** • Ports des Administrationsservers für die Verbindung mit mobilen Geräten angeben: **Schreiben** • Maximale Anzahl von Ereignissen, die in der Administrationsserver-Datenbank gespeichert sind, angeben: **Schreiben** • Maximale Anzahl von Ereignissen, die der Administrationsserver versenden kann, angeben: **Schreiben** • Zeitspanne, in welcher Ereignisse durch den Administrationsserver versendet werden können, angeben: **Schreiben**	• "Backup der Daten des Administrationsservers anlegen" • "Pflege von Datenbanken"	Nichts
Allgemeine Funktionen: **Verteilung von Programmen von Kaspersky**	• **Patches von Kaspersky verwalten** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	Die Installation von Patches akzeptieren oder ablehnen: **Patches von Kaspersky verwalten**	Nichts	• "Bericht über Lizenzschlüs des virtueller Administratio • "Bericht über der Kaspersk Programme" • "Bericht über inkompatible Anwendunge

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
				• "Bericht über Versionen de Kaspersky-P Module" • "Bericht über Bereitstellun Schutzes"
Allgemeine Funktionen: **Schlüsselverwaltung**	• **Schlüsseldatei exportieren** • **Schreiben**	• Schlüsseldatei exportieren: **Schlüsseldatei exportieren** • Einstellungen des Lizenzschlüssels des Administrationsservers ändern: **Schreiben**	Nichts	Nichts
Allgemeine Funktionen: **Erzwungene Berichtsverwaltung**	• **Lesen** • **Schreiben**	• Berichte unabhängig von ihren ACLs erstellen: **Schreiben** • Berichte unabhängig von ihren ACLs exportieren: **Lesen**	Nichts	Nichts
Allgemeine Funktionen: **Hierarchie von Administrationsservern**	**Hierarchie von Administrationsservern konfigurieren**	• Sekundäre Administrationsserver registrieren, aktualisieren oder löschen: **Hierarchie von Administrationsservern konfigurieren**	Nichts	Nichts
Allgemeine Funktionen: **Benutzerrechte**	**Objekt-ACLs ändern**	• "Sicherheit"-Eigenschaften eines jeden Objekts ändern: **Objekt-ACLs ändern** • Benutzerrollen verwalten: **Objekt-ACLs ändern** • Interne Benutzer verwalten: **Objekt-ACLs ändern** • Sicherheitsgruppen verwalten: **Objekt-ACLs ändern** • Anmeldenamen verwalten: **Objekt-ACLs ändern**	Nichts	Nichts
Allgemeine Funktionen: **Virtuelle Administrationsserver**	• **Virtuelle Administrationsserver verwalten** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Liste mit virtuellen Administrationsservern abrufen: **Lesen** • Informationen über den virtuellen Administrationsserver erhalten: **Lesen** • Virtuellen Administrationsserver erstellen, aktualisieren oder löschen: **Virtuelle Administrationsserver verwalten** • Virtuellen Administrationsserver in andere Gruppe verschieben: **Virtuelle Administrationsserver verwalten** • Rechte des virtuellen Administrationsservers angeben: **Virtuelle Administrationsserver verwalten**	Nichts	Nichts

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
Allgemeine Funktionen: **Verwaltung der Chiffrierschlüssel**	**Schreiben**	Importieren von Chiffrierschlüsseln: **Schreiben**	Nichts	Nichts
Verwaltung mobiler Geräte: **Allgemein**	• **Neue Geräte verbinden** • **Nur Informationsbefehle an mobile Geräte senden** • **Befehle an mobile Geräte senden** • **Zertifikate verwalten** • **Lesen** • **Schreiben**	• Wiederherstellungsdaten des Schlüsselverwaltungsdienstes abrufen **Read** • Benutzerzertifikate löschen: **Zertifikate verwalten** • Öffentlichen Teil eines Benutzerzertifikats abrufen: **Lesen** • Aktivierung der Public-Key-Infrastruktur prüfen: **Lesen** • Konto der Public-Key-Infrastruktur prüfen: **Lesen** • Vorlagen der Public-Key-Infrastruktur abrufen: **Lesen** • Vorlagen der Public-Key-Infrastruktur nach Zertifikat der "Extended Key Usage" abrufen: **Lesen** • Widerruf des Zertifikats der Public-Key-Infrastruktur prüfen: **Lesen** • Einstellungen für die Ausstellung von Benutzerzertifikaten aktualisieren: **Zertifikate verwalten** • Einstellungen für die Ausstellung von Benutzerzertifikaten abrufen: **Lesen** • Pakete nach Programmname und Version abrufen: **Lesen** • Benutzerzertifikate einstellen oder abbrechen: **Zertifikate verwalten** • Benutzerzertifikate erneuern: **Zertifikate verwalten** • Tags für Benutzerzertifikate einstellen: **Zertifikate verwalten** • Erzeugung von MDM-Installationspaketen ausführen / abbrechen: **Neue Geräte verbinden**	Nichts	Nichts
Systemverwaltung: **Verbindungen**	• **RDP-Sitzungen starten** • **Zu bestehenden RDP-Sitzungen verbinden** • **Tunnelung initiieren** • **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern** • **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Desktop-Sharing-Sitzung erstellen: **Das Recht zum Erstellen einer Desktop-Sharing-Sitzung** • RDP-Sitzungen erstellen: **Zu bestehenden RDP-Sitzungen verbinden** • Tunnel erstellen: **Tunnelung initiieren** • Liste mit Content-Netzwerken speichern: **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern**	Nichts	"Bericht über Gerätebenutzer"
Systemverwaltung: **Schwachstellen- und Patch-Management**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Eigenschaften von Patches von Drittanbietern anzeigen: **Lesen** • Eigenschaften von Patches von Drittanbietern ändern: **Schreiben**	• "Schwachstellen schließen" • "Erforderliche Updates installieren und Schwachstellen schließen"	"Bericht über Pro Updates"
Systemverwaltung: **Remote-Ausführung von Skripten**	• **Lesen** • **Schreiben**	Der Benutzer kann die Aufgabeneigenschaften anzeigen: **Lesen**	"Remote-Ausführung von Skripten"	Keine

Funktionsbereich	Berechtigung	Benutzervorgang: benötigte Berechtigung, um den Vorgang auszuführen	Aufgabe	Bericht
	• **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	Der Benutzer kann ein Installationspaket erstellen, löschen oder ändern: **Schreiben** Der Benutzer kann eine Aufgabe starten: **Schreiben**. Auf Client-Geräten unter Linux werden Skripte mit Root-Rechten ausgeführt. Der Benutzer kann eine Aufgabe ausführen oder deren Ausführung planen: **Ausführen** Der Benutzer kann eine Aufgabe auf einer Auswahl von Geräten ausführen: **Vorgänge für die Geräteauswahlen ausführen**		

Vorkonfigurierte Benutzerrollen

Benutzer von Kaspersky Security Center Linux mit zugewiesenen Benutzerrollen bekommen Zugriffsrechte auf Anwendungsfunktionen gewährt.

Benutzern, die auf einem virtuellen Server erstellt wurden, können auf dem Administrationsserver keine Rollen zugewiesen werden.

Sie können entweder vordefinierte Benutzerrollen mit bereits festgelegten Zugriffsrechten verwenden oder neue Rollen erstellen. Beim Erstellen einer neuen Rolle müssen Sie den Gültigkeitsbereich der Rolle festlegen und die Zugriffsberechtigungen auf die Funktionen von Kaspersky Security Center Linux selbst zuweisen. Einige der in Kaspersky Security Center Linux verfügbaren vordefinierten Benutzerrollen können bestimmten Positionen zugeordnet werden, z. B. **Auditor**, **Sicherheitsbeauftragter** oder **Supervisor**. Die Zugriffsberechtigungen dieser Rollen wurden gemäß den Standardaufgaben und den Tätigkeitsbereichen der entsprechenden Positionen vorkonfiguriert. Die folgende Tabelle gibt an, wie Rollen mit spezifischen beruflichen Positionen verbunden werden können.

Beispiele von Rollen für spezifische berufliche Positionen

Rolle	Kommentar
Auditor	Erlaubt alle Anzeigevorgänge und die Ausführung aller erstellten Aufgaben auf ausgewählten Geräten, die mit dem Administrationsserver über den Administrationsagenten mit lokalen Administratorrechten (root für Linux) verbunden sind. Es wird empfohlen, diese Rolle umsichtig zu gewähren und nur einer begrenzten Anzahl von Benutzern zuzuweisen, die diese Rechte zur Erfüllung ihrer offiziellen Verpflichtungen benötigen.
Supervisor	Erlaubt alle Anzeige-Vorgänge, erlaubt keine anderen Vorgänge. Sie können diese Rolle einem Security Officer und anderen Verantwortlichen zuweisen, die für die IT-Sicherheit in Ihrer Organisation zuständig sind.
Security Officer	Erlaubt alle Anzeige-Vorgänge, erlaubt Berichtsverwaltung; gewährt eingeschränkte Beschränkungen im Bereich **Systemverwaltung**: **Konnektivität**. Sie können diese Rolle einem Beauftragten zuweisen, der für die IT-Sicherheit in Ihrer Organisation zuständig ist.

Die folgende Tabelle gibt die jeder vorkonfigurierten Benutzerrolle zugewiesenen Zugriffsberechtigungen an.

Zugriffsberechtigungen von vorkonfigurierten Benutzerrollen

Rolle	Beschreibung
Administrator des Administrationsserver	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Verwaltung der Chiffrierschlüssel** • **Verarbeitung von Ereignissen** • **Hierarchie des Administrationsservers** • **Virtuelle Administrationsserver** • **Systemverwaltung**: • **Konnektivität** • **Hardware-Inventarisierung** • **Software-Inventur**
Operator des Administrationsserver	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Verwaltung der Chiffrierschlüssel** • **Virtuelle Administrationsserver** • **Systemverwaltung**: • **Konnektivität** • **Hardware-Inventarisierung** • **Software-Inventur**
Auditor	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen in **Allgemeine Funktionen**: • **Zugriff auf Objekte, unabhängig von deren ACLs** • **Gelöschte Objekte** • **Erzwungene Berichtsverwaltung** Sie können diese Rolle einer Person zuweisen, die das Audit Ihres Unternehmens durchführt.
Installationsadministrator	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen:** • **Grundlegende Funktionen** • **Kaspersky-Anwendungsbereitstellung** • **Verwaltung von Lizenzschlüsseln** • **Systemverwaltung:** • **Bereitstellung des Betriebssystems** • **Schwachstellen- und Patch-Management** • **Remote-Installation** • **Software-Inventur** Gewährt die Berechtigungen **Lesen** und **Ausführen** in dem Funktionsbereich **Allgemeine Funktionen: Virtuelle Administrationsserver**.

Rolle	Beschreibung
Installationsoperator	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen:** • **Grundlegende Funktionen** • **Bereitstellung der Anwendungen von Kaspersky** (gewährt auch die Berechtigung **Verwaltung der Patches von Kaspersky** in diesem Bereich) • **Virtuelle Administrationsserver** • **Systemverwaltung:** • **Bereitstellung des Betriebssystems** • **Schwachstellen- und Patch-Management** • **Remote-Installation** • **Software-Inventur**
Administrator von Kaspersky Endpoint Security	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel** • Alle Funktionen aus dem Bereich von **Kaspersky Endpoint Security**
Operator von Kaspersky Endpoint Security	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel** • Alle Funktionen aus dem Bereich von **Kaspersky Endpoint Security**
Hauptadministrator	Gewährt alle Vorgänge in Funktionsbereichen, *außer* für die folgenden Bereiche in **Allgemeine Funktionen**: • **Zugriff auf Objekte, unabhängig von deren ACLs** • **Erzwungene Berichtsverwaltung**
Hauptoperator	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Gelöschte Objekte** • **Verwaltung der Chiffrierschlüssel** • **Vorgänge auf dem Administrationsserver** • **Geräte-Tags** • **Bereitstellung der Anwendungen von Kaspersky** • **Anwendungsintegration** • **Virtuelle Administrationsserver** • Alle Funktionen aus dem Bereich von **Verwaltung mobiler Geräte** • Alle Funktionen aus dem Bereich von **Systemverwaltung** • Alle Funktionen aus dem Bereich von **Kaspersky Endpoint Security**
Administrator der Funktion "Verwaltung mobiler Geräte"	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • Alle Funktionen aus dem Bereich von **Verwaltung mobiler Geräte** Gewährt die Berechtigung **Export der Schlüsseldatei** in **Allgemeine Funktionen: Lizenzschlüsselverwaltung**. Gewährt die Berechtigung **Lesen** in der **Systemverwaltung: Schwachstellen- und Patch-Management**.
Operator der Funktion "Verwaltung mobiler Geräte"	Gewährt die Berechtigungen **Lesen** und **Ausführen** in **Allgemeine Funktionen: Grundlegende Funktionen**. Gewährt die Berechtigungen **Lesen** und **Nur Informationsbefehle an mobile Geräte senden** in der **Verwaltung mobiler Geräte**: • **Allgemein** • **Self Service Portal**

Rolle	Beschreibung
Security Officer	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen in **Allgemeine Funktionen**: • **Zugriff auf Objekte, unabhängig von deren ACLs** • **Erzwungene Berichtsverwaltung** Gewährt die folgenden Berechtigungen im Funktionsbereich **Systemverwaltung: Verbindungen**: **Lesen**, **Schreiben**, **Ausführen**, **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern** und **Vorgänge auf Geräteauswahlen ausführen**. Sie können diese Rolle einem Beauftragten zuweisen, der für die IT-Sicherheit in Ihrer Organisation zuständig ist.
Benutzer des Self Service Portals	Erlaubt alle Vorgänge im Funktionsbereich **Verwaltung mobiler Geräte: Self Service Portal**.
Supervisor	Gewährt die Berechtigung **Lesen** in den Funktionsbereichen **Allgemeine Funktionen**: **Zugriff auf Objekte, unabhängig von ihren ACLs** und **Allgemeine Funktionen**: **Erzwungene Berichtsverwaltung**. Sie können diese Rolle einem Security Officer und anderen Verantwortlichen zuweisen, die für die IT-Sicherheit in Ihrer Organisation zuständig sind.
Administrator der Funktionen "Schwachstellen- und Patch-Management"	Erlaubt alle Vorgänge in den Funktionsbereichen **Allgemeine Funktionen**:**Grundlegende Funktionalität** und **Systemverwaltung** (einschließlich aller Funktionen *außer* der Funktion **Remote-Ausführung von Skripten**).
Operator der Funktionen "Schwachstellen- und Patch-Management"	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in den Funktionsbereichen **Allgemeine Funktionen**: **Grundlegende Funktionalität** und **Systemverwaltung** (einschließlich aller Funktionen *außer* der Funktion **Remote-Ausführung von Skripten**).

Bestimmten Objekten Zugriffsrechte zuweisen

Neben der Zuweisung von Zugriffsrechten auf Ebene von Funktionsbereichen können Sie auch den Zugriff auf bestimmte Objekte konfigurieren, beispielsweise einer bestimmten Administrationsgruppe oder Aufgabe. Mit der Anwendung können Sie Zugriffsrechte für die folgenden Objekttypen festlegen:

- Administrationsgruppen
- Aufgaben
- Berichte
- Geräteauswahlen
- Ereignisauswahlen

So weisen Sie einem bestimmten Objekt Zugriffsrechte zu:

1. Gehen Sie je nach Objekttyp im Hauptmenü zum entsprechenden Abschnitt:
   - **Asset-Verwaltung → Gruppenhierarchie**
   - **Aufgaben**
   - **Überwachung → Berichte**
   - **Asset-Verwaltung → Geräteauswahlen**
   - **Überwachung → Ereignisauswahlen**

2. Öffnen Sie die Eigenschaften des Objekts, für das Sie Zugriffsrechte konfigurieren möchten.

   Um das Eigenschaftsfenster einer Administrationsgruppe oder einer Aufgabe zu öffnen, klicken Sie auf den Objektnamen. Eigenschaften anderer Objekte können über die Schaltfläche in der Werkzeugleiste geöffnet werden.

3. Gehen Sie im Eigenschaftenfenster zum Abschnitt **Zugriffsrechte**.

   Die Benutzerliste wird geöffnet. Die aufgelisteten Benutzer und Sicherheitsgruppen haben Zugriffsrechte auf das Objekt. Wenn Sie eine Hierarchie von Administrationsgruppen oder Servern verwenden, werden die Liste und die Zugriffsrechte standardmäßig von der übergeordneten Administrationsgruppe oder dem primären Server übernommen.

4. Um die Liste ändern zu können, aktivieren Sie die Option **Benutzerdefinierte Berechtigungen verwenden**.

5. Konfigurieren der Zugriffsrechte:

   - Verwenden Sie die Schaltflächen **Hinzufügen** und **Löschen**, um die Liste zu ändern.
   - Geben Sie für einen Benutzer oder eine Sicherheitsgruppe die Zugriffsrechte an. Führen Sie eine der folgenden Aktionen aus:
     - Wenn Sie Zugriffsrechte manuell festlegen möchten, wählen Sie den Benutzer oder die Sicherheitsgruppe aus, klicken Sie auf die Schaltfläche **Zugriffsrechte** und legen Sie anschließend die Zugriffsrechte fest.
     - Wenn Sie einem Benutzer oder einer Sicherheitsgruppe eine Benutzerrolle zuweisen möchten, wählen Sie den Benutzer oder die Sicherheitsgruppe aus, klicken Sie auf die Schaltfläche **Rollen** und wählen Sie anschließend die zuzuweisende Rolle aus.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Die Zugriffsrechte auf das Objekt sind konfiguriert.

Zuweisung von Zugriffsrechten an Benutzer und Sicherheitsgruppen

Sie können Benutzern und Sicherheitsgruppen Zugriffsrechte für die Nutzung verschiedener Funktionen des Administrationsservers zuweisen, z. B. für Kaspersky Endpoint Security für Linux.

So weisen Sie einem Benutzer oder einer Sicherheitsgruppe Zugriffsrechte zu:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Zugriffsrechte** das Kontrollkästchen neben dem Namen des Benutzers oder der Sicherheitsgruppe, dem bzw. der Rechte zugewiesen werden sollen, und klicken Sie dann auf die Schaltfläche **Zugriffsrechte**.

   Sie können nur einzelne Benutzer oder Sicherheitsgruppen auswählen. Wenn Sie mehr als ein Element auswählen, wird die Schaltfläche **Zugriffsrechte** deaktiviert.

3. Konfigurieren Sie die erforderlichen Rechte für den Benutzer oder die Gruppe:

   a. Erweitern Sie den Knoten mit den Funktionen des Administrationsservers oder einer anderen Kaspersky-Anwendung.

   b. Aktivieren Sie neben der gewünschten Funktion oder dem gewünschten Zugriffsrecht das Kontrollkästchen **Zulassen** oder **Verbieten**.

      Beispiel 1: Aktivieren Sie das Kontrollkästchen **Erlauben** neben dem Knoten **Anwendungsintegration**, um einem Benutzer oder einer Gruppe alle verfügbaren Zugriffsrechte für die Funktionen der Anwendungsintegration (**Lesen**, **Schreiben** und **Ausführen**) zu gewähren.

      Beispiel 2: Erweitern Sie den Knoten **Verwaltung von Chiffrierschlüsseln** und aktivieren Sie das Kontrollkästchen **Erlauben** neben **Schreibzugriff**, um einem Benutzer oder einer Gruppe das Zugriffsrecht **Schreiben** für die Funktion zur Verwaltung von Chiffrierschlüsseln zu gewähren.

4. Klicken Sie nach der Konfiguration der Zugriffsrechte auf **OK**.

Die Auswahl der Rechte für den Benutzer oder die Benutzergruppe wird angepasst.

Die Berechtigungen des Administrationsservers (oder der Administrationsgruppe) sind in die folgenden Bereiche unterteilt:

- Allgemeine Funktionen:
  - Verwaltung von Administrationsgruppen
  - Auf Objekte unabhängig von ihren ACLs zugreifen
  - Basisfunktionen
  - Gelöschte Objekte
  - Verwaltung der Chiffrierschlüssel
  - Verarbeitung von Ereignissen
  - Vorgänge mit dem Administrationsserver (nur im Eigenschaftsfenster des Administrationsservers)
  - Tags des Geräts
  - Bereitstellen von Kaspersky-Anwendungen
  - Lizenzschlüsselverwaltung
  - Anwendungsintegration
  - Erzwungene Berichtsverwaltung
  - Hierarchie der Administrationsserver
  - Benutzerberechtigungen
  - Virtuelle Administrationsserver

- Verwaltung mobiler Geräte:
  - Allgemein
  - Self Service Portal
- Systemverwaltung:
  - Konnektivität
  - Skripte remote ausführen
  - Hardware-Inventur
  - Network Access Control (NAC)
  - Bereitstellung des Betriebssystems
  - Schwachstellen- und Patch-Management
  - Remote-Installation
  - Software-Inventur

Wenn für ein Zugriffsrecht weder **Zulassen** noch **Verbieten** ausgewählt ist, gilt das Zugriffsrecht als *Nicht festgelegt*: Der Zugriff wird verweigert, bis er für den Benutzer ausdrücklich verweigert oder erlaubt wird.

Die Rechte eines Benutzers setzen sich aus folgenden Faktoren zusammen:

- Eigene Rechte des Benutzers
- Rechte aller Rollen, die diesem Benutzer zugewiesen sind
- Rechte aller Sicherheitsgruppen, zu denen der Benutzer gehört
- Rechte aller Rollen, die den Sicherheitsgruppen zugewiesen sind, zu denen der Benutzer gehört

Wenn zumindest einer dieser Faktoren für eine Berechtigung den Status **Verbieten** hat, wird dem Benutzer diese Berechtigung verweigert, selbst wenn sie für andere Faktoren erlaubt oder nicht festgestellt ist.

Sie können auch Benutzer und Sicherheitsgruppen zum Umfang einer Benutzerrolle hinzufügen, um verschiedene Funktionen des Administrationsservers zu nutzen. Einstellungen, die einer Benutzerrolle zugeordnet sind, gelten nur für jene Geräte, die den Benutzern gehören, die diese Rolle innehaben, und nur, wenn diese Geräte zu Gruppen gehören, die mit dieser Rolle verknüpft sind, einschließlich Untergruppen.

Benutzerkonto für einen internen Benutzer hinzufügen

Wenn Sie ein Benutzerkonto hinzufügen möchten, stellen Sie sicher, dass Ihr Konto die Berechtigung Objekt-ACLs ändern in dem Funktionsbereich "Allgemeine Funktionen: Benutzerberechtigungen" besitzt.

Um ein neues internes Benutzerkonto zu Kaspersky Security Center Linux hinzuzufügen:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im folgenden Fenster **Benutzer hinzufügen** die Einstellungen des neuen Benutzerkontos an:
   - **Name**.
   - **Kennwort** für die Verbindung des Benutzers mit Kaspersky Security Center Linux.

     Das Kennwort muss den folgenden Regeln entsprechen:
     - Das Kennwort muss zwischen 8 und 256 Zeichen lang sein.
     - Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
       - Großbuchstaben (A–Z)
       - Kleinbuchstaben (a–z)
       - Ziffern (0–9)
       - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

     Um das eingegebene Kennwort anzuzeigen, klicken Sie auf .

     Sie können die Option **Benutzer muss bei Erstanmeldung sein Kennwort ändern** aktivieren, um bei der ersten Authentifizierung eines Benutzers eine Änderung des Kennworts zu erzwingen.
4. Speichern Sie die Änderungen, um die Erstellung des neuen Benutzerkontos abzuschließen.

Ein neues Benutzerkonto wird zur Liste mit Benutzern hinzugefügt.

Um sich mit einem erstellten internen Benutzerkonto an der Kaspersky Security Center Web Console anzumelden, müssen Sie diesem Konto eine Rolle zuweisen. Stellen Sie vor der Anmeldung sicher, dass dem internen Benutzerkonto eine Rolle zugewiesen wurde. Andernfalls tritt ein Anmeldefehler auf.

Eine Sicherheitsgruppe erstellen

Um eine Sicherheitsgruppen zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Gruppen** aus.
2. Klicken Sie auf **Hinzufügen**.

3. Nehmen Sie im folgenden Fenster **Sicherheitsgruppe erstellen** die folgenden Einstellungen für die neue Sicherheitsgruppe vor:

   - **Gruppenname**
   - **Beschreibung**

4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Eine neue Sicherheitsgruppe wird zur Liste mit Gruppen hinzugefügt.

Benutzerkonto eines internen Benutzers bearbeiten

Wenn Sie ein Benutzerkonto bearbeiten möchten, stellen Sie sicher, dass Ihr Konto die Berechtigung Objekt-ACLs ändern in dem Funktionsbereich "Allgemeine Funktionen: Benutzerberechtigungen" besitzt.

Um ein internes Benutzerkonto in Kaspersky Security Center Linux zu bearbeiten:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Klicken Sie auf den Namen des Benutzerkontos, das Sie bearbeiten möchten.
3. Ändern Sie im folgenden Fenster für Benutzereinstellungen auf der Registerkarte **Allgemein** die Einstellungen für das Benutzerkonto:

   - **Benutzerkonto**

     Schalten Sie ggf. die Umschalttaste auf **Inaktiv**, um zu verhindern, dass der Benutzer eine Verbindung zur Anwendung herstellt. Sie können ein Konto beispielsweise deaktivieren, nachdem ein Mitarbeiter das Unternehmen verlassen hat.

   - Beschreibung
   - **Vollständiger Name**
   - **E-Mail-Adresse**
   - **Hauptrufnummer**
   - **Kennwort**

     Bei Bedarf können Sie für die Verbindung des Benutzers zu Kaspersky Security Center Linux ein neues Kennwort wie folgt festlegen:

     a. Klicken Sie auf die Schaltfläche **Kennwort ändern** und legen Sie anschließend ein neues Kennwort für das Benutzerkonto fest.

Das Kennwort muss den folgenden Regeln entsprechen:

- Das Kennwort muss zwischen 8 und 256 Zeichen lang sein.
- Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
  - Großbuchstaben (A–Z)
  - Kleinbuchstaben (a–z)
  - Ziffern (0–9)
  - Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

Um das eingegebene Kennwort anzuzeigen, klicken Sie auf .

b. Bei Bedarf können Sie die Option **Benutzer muss bei Erstanmeldung sein Kennwort ändern** aktivieren, um bei der nächsten Authentifizierung eines Benutzers eine Änderung des Kennworts zu erzwingen.

c. Wenn das Benutzerkonto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie über die Berechtigungen zur Kontoänderung verfügen. Geben Sie im Fenster **Schutz des Benutzerkontos** die Anmeldeinformationen des Benutzerkontos an, das über die Berechtigung Objekt-ACL ändern im Funktionsbereich "Allgemeine Funktionen: Benutzerberechtigungen" verfügt.

4. Auf der Registerkarte **Zwei-Faktor-Authentifizierung** können Sie die Sicherheitseinstellungen für dieses Benutzerkonto festlegen.
5. Auf der Registerkarte **Gruppen** können Sie einen Benutzer zu Sicherheitsgruppen hinzufügen.
6. Auf der Registerkarte **Geräte** können Sie einem Benutzer Geräte zuweisen.
7. Auf der Registerkarte **Rollen** können Sie einem Benutzer Rollen zuordnen.
8. Speichern Sie die Änderungen, um die Bearbeitung des Benutzerkontos abzuschließen.

Das aktualisierte Benutzerkonto wird in der Liste der Benutzer angezeigt.

Eine Sicherheitsgruppe bearbeiten

So bearbeiten Sie eine Sicherheitsgruppe:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Gruppen** aus.
2. Klicken Sie auf den Namen der Sicherheitsgruppe, die Sie bearbeiten möchten.

3. Ändern Sie im folgenden Fenster mit den Gruppeneinstellungen die Einstellungen für die Sicherheitsgruppe:

   - Auf der Registerkarte **Allgemein** können Sie die Einstellungen **Name** und **Beschreibung** ändern. Diese Einstellungen sind nur für interne Sicherheitsgruppen verfügbar.
   - Auf der Registerkarte **Benutzer** können Sie Benutzer zur Sicherheitsgruppe hinzufügen. Diese Einstellung ist nur für interne Benutzer und interne Sicherheitsgruppen verfügbar.
   - Auf der Registerkarte **Rollen** können Sie einer Sicherheitsgruppe eine Rolle zuweisen.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Änderungen werden auf die Sicherheitsgruppe angewendet.

Einem Benutzer oder einer Sicherheitsgruppe eine Rolle zuweisen

So weisen Sie einem Benutzer oder einer Sicherheitsgruppe eine Rolle zu:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** oder **Gruppen** aus.
2. Wählen Sie den Namen des Benutzers oder der Sicherheitsgruppe aus, dem oder der Sie die Rolle zuweisen wollen.

   Es können mehrere Namen ausgewählt werden.
3. Klicken Sie in der Menüleiste auf die Schaltfläche **Rolle zuordnen**.

   Der Assistent zum Zuweisen einer Rolle wird gestartet.
4. Folgen Sie den Anweisungen des Assistenten: Wählen Sie die Rolle aus, die Sie den ausgewählten Benutzern oder Sicherheitsgruppen zuweisen wollen, und legen Sie anschließend den Gültigkeitsbereich der Rolle fest.

   Ein *Benutzerrollenbereich* ist eine Kombination von Benutzern und Administrationsgruppen. Einstellungen, die mit einer Benutzerrolle verbunden sind, gelten nur für Geräte, die Benutzern gehören, die über diese Rolle verfügen, und nur, wenn diese Geräte zu Gruppen gehören, die mit dieser Rolle verbunden sind, einschließlich untergeordnete Gruppen.

Als Ergebnis wird dem Benutzer, den Benutzern oder der Sicherheitsgruppe die Rolle mit einer Auswahl von Berechtigungen für die Arbeit mit dem Administrationsserver zugewiesen. In der Liste der Benutzer oder Sicherheitsgruppen wird in der Spalte **Zugeordnete Rollen** ein Kontrollkästchen angezeigt.

Benutzerkonten zu einer internen Sicherheitsgruppe hinzufügen

Einer internen Sicherheitsgruppe können nur die Benutzerkonten von internen Benutzern hinzugefügt werden.

So fügen Sie einer internen Sicherheitsgruppe Benutzerkonten hinzu:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Aktivieren Sie die Kontrollkästchen neben den Benutzerkonten, die Sie einer Sicherheitsgruppe hinzufügen möchten.
3. Klicken Sie auf die Schaltfläche **Gruppe zuordnen**.
4. Wählen Sie im folgenden Fenster **Gruppe zuordnen** die Sicherheitsgruppe aus, der Sie die Benutzerkonten hinzufügen möchten.
5. Klicken Sie auf **Speichern**.

Die Benutzerkonten werden der Sicherheitsgruppe hinzugefügt. Sie können interne Benutzer auch mithilfe der Gruppeneinstellungen zu einer Sicherheitsgruppe hinzufügen.

Benutzer zu Gerätebesitzern ernennen

Weitere Informationen darüber, wie man einen Benutzer zum Gerätebesitzer macht, entnehmen Sie der Hilfe von Kaspersky Secure Mobility Management.

So machen Sie einen Benutzer zum Gerätebesitzer:

1. Wenn Sie einem Gerät, das mit einem virtuellen Administrationsserver verbunden ist, einen Besitzer zuweisen möchten, wechseln Sie zunächst zum virtuellen Administrationsserver:
   a. Klicken Sie im Hauptmenü rechts neben dem Namen des aktuellen Administrationsservers auf das Chevron-Symbol ( ).
   b. Wählen Sie den gewünschten Administrationsserver aus.
2. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.

   Die Liste mit Benutzern wird geöffnet. Wenn Sie derzeit mit einem virtuellen Administrationsserver verbunden sind, enthält die Liste die Benutzer des aktuellen virtuellen Administrationsservers sowie des primären Administrationsservers.
3. Klicken Sie auf den Namen des Benutzerkontos, das Sie als Gerätebesitzer zuweisen möchten.
4. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Geräte**.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**.
6. Wählen Sie in der Geräteliste die Richtlinie aus, die Sie dem Benutzer zuweisen möchten.
7. Klicken Sie auf die Schaltfläche **OK**.

Das ausgewählte Gerät wird zur Liste der dem Benutzer zugewiesenen Geräte hinzugefügt.

Derselbe Vorgang kann auch unter **Asset-Verwaltung** → **Assets (Geräte)** ausgeführt werden: Klicken Sie auf den Namen des Geräts, das Sie zuweisen möchten, und klicken Sie dann auf den Link **Gerätebesitzer verwalten**.

Benutzer während der Installation des Administrationsagenten zum Gerätebesitzer ernennen

Um einen Benutzer während der Installation des Administrationsagenten mithilfe eines Installationspakets zum Gerätebesitzer zu ernennen, fügen Sie die in der folgenden Tabelle angegebenen Variablen zu den Einstellungen des Installationspakets für den Administrationsagenten hinzu.

Name der Variablen	Erforderlich	Beschreibung	Mögliche Werte
KLNAGENT_DEVICEOWNER_REGISTRATION_START	Nein	Ermöglicht die Ausführung des Tools zur Registrierung des Benutzers als Gerätebesitzer nach der Installation des Administrationsagenten. Bei deaktivierter Option ist die Registrierung als Gerätebesitzer für Benutzer nicht verfügbar.	1 – Das Tool zur Registrierung des Benutzers als Gerätebesitzer wird nach der Installation des Administrationsagenten gestartet. Anderer Wert – Das Tool ist nicht verfügbar.
KLNAGENT_DEVICEOWNER_LOGIN	Nein Ja, wenn Sie das Kennwort eingeben	Enthält den Benutzernamen eines Benutzers, der als Gerätebesitzer registriert wird.	Der Benutzername des Benutzers, wie er in der Benutzerliste in Kaspersky Security Center Linux angegeben ist.
KLNAGENT_DEVICEOWNER_PASSWORD	Nein Ja, wenn Sie den Benutzernamen eingeben	Enthält das verschlüsselte Kennwort eines Benutzers, der als Gerätebesitzer registriert wird.	Das Kennwort des Benutzers.

Der Administrationsagent entschlüsselt während der Installation von Kaspersky Security Center Linux den angegebenen Benutzernamen und das Kennwort, und der Benutzer wird als Gerätebesitzer registriert.

Sie können einen Benutzer auch zum Gerätebesitzer ernennen, wenn Sie den Administrationsagenten im Silent-Modus mit einer Antwortdatei installieren.

So ernennen Sie einen Benutzer zum Gerätebesitzer, während der Administrationsagent im Silent-Modus mit einer Antwortdatei installiert wird:

1. Fügen Sie der Antwortdatei den Parameter KLNAGENT_DEVICEOWNER_REGISTRATION_START hinzu und setzen Sie ihn auf "1".

   Das Tool zur Registrierung des Benutzers als Gerätebesitzer wird nach der Installation des Administrationsagenten gestartet.

2. Geben Sie den Benutzernamen und das Kennwort in die Befehlszeile des Client-Geräts ein.

   Der Benutzer wird zum Gerätebesitzer ernannt.

Wenn der Benutzer zu einer internen Sicherheitsgruppe gehört, muss die Anmeldung den Benutzernamen enthalten.

Wenn der Benutzer zu einer Active Directory-Sicherheitsgruppe gehört, muss die Anmeldung den Benutzernamen und den Domänennamen enthalten.

Sie müssen das zeitbasierte Einmalkennwort (TOTP) aus der App eingeben für Zwei-Faktor-Authentifizierung.

Benutzer nach der Installation des Administrationsagenten zum Linux-Gerätebesitzer ernennen

So erlauben Sie dem Benutzer, sich als Linux-Gerätebesitzer zu registrieren:

1. Gehen Sie in der Kaspersky Security Center Web Console zu **Software-Verwaltung** → **Installationspakete**.

   Die Liste der Installationspakete wird geöffnet.

2. Klicken Sie auf das Installationspaket des Administrationsagenten.

   Das Eigenschaftenfenster des Installationspakets wird geöffnet.

3. Klicken Sie im Eigenschaftenfenster des Installationspakets auf **Einstellungen** → **Erweitert**.

4. Aktivieren Sie im Abschnitt **Benutzerregistrierung als Gerätebesitzer (nur Linux)** die Option **Ausführen des Tools zur Benutzerregistrierung nach Installation des Administrationsagenten zulassen** und klicken Sie auf **Speichern**.

Das Tool zur Benutzerregistrierung als Gerätebesitzer kann über die Befehlszeile auf dem Client-Gerät ausgeführt werden.

So ernennen Sie einen Benutzer zum Linux-Gerätebesitzer des Client-Geräts:

1. Führen Sie in der Befehlszeile des Client-Geräts den folgenden Befehl aus:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Geben Sie bei Aufforderung den Benutzernamen und das Kennwort ein.

   Wenn der Benutzername und das Kennwort in der Antwortdatei oder im Installationspaket des Administrationsagenten enthalten sind, führen Sie in der Befehlszeile des Client-Geräts den folgenden Befehl aus:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Wenn der Benutzer zu einer internen Sicherheitsgruppe gehört, muss die Anmeldung den Benutzernamen enthalten.

Wenn der Benutzer zu einer Active Directory-Sicherheitsgruppe gehört, muss die Anmeldung den Benutzernamen und den Domänennamen enthalten.

Sie müssen das zeitbasierte Einmalkennwort (TOTP) aus der App eingeben für Zwei-Faktor-Authentifizierung.

Der Benutzer wird als Gerätebesitzer registriert.

Benutzer als Gerätebesitzer entfernen

So entfernen Sie einen Benutzer als Gerätebesitzer eines Client-Geräts:

1. Führen Sie in der Befehlszeile den folgenden Befehl aus:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -remove_owner
   ```

2. Geben Sie den Benutzernamen und das Kennwort ein.

Wenn der Benutzer zu einer internen Sicherheitsgruppe gehört, muss die Anmeldung den Benutzernamen enthalten.

Wenn der Benutzer zu einer Active Directory-Sicherheitsgruppe gehört, muss die Anmeldung den Benutzernamen und den Domänennamen enthalten.

Sie müssen das zeitbasierte Einmalkennwort (TOTP) aus der App eingeben für Zwei-Faktor-Authentifizierung.

Der Benutzer wird als Gerätebesitzer entfernt.

Aktivieren des Benutzerkonten-Schutzes vor unbefugten Änderungen

Sie können eine zusätzliche Option aktivieren, um ein Benutzerkonto vor unbefugten Änderungen zu schützen. Wenn diese Option aktiviert ist, muss sich der Benutzer mit Änderungsrechten autorisieren, um die Benutzerkonto-Einstellungen zu ändern.

So aktivieren oder deaktivieren Sie den Benutzerkonten-Schutz vor unbefugten Änderungen:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.

2. Klicken Sie auf den Namen des internen Benutzerkontos, für das Sie den Benutzerkonten-Schutz vor nicht autorisierten Änderungen anpassen möchten.

3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Zwei-Faktor-Authentifizierung**.

4. Auf der Registerkarte **Zwei-Faktor-Authentifizierung**, wählen Sie die Option **Authentifizierung erfordern, um zu prüfen, ob Benutzerkonten geändert werden dürfen**, wenn Sie bei jeder Änderung oder Modifizierung der Kontoeinstellungen Anmeldedaten und einen Einmal-Sicherheitscode für die Zwei-Faktor-Authentifizierung anfordern möchten. Wählen Sie andernfalls die Option **Benutzern das Ändern des Kontos ohne zusätzliche Authentifizierung erlauben**.

5. Speichern Sie die Änderungen.

Konfigurieren Sie die Zwei-Faktor-Authentifizierung

Beginnend mit der Administrationsserver-Version 16.1, Zwei-Faktor-Authentifizierung wird automatisch aktiviert. Die globale Option zum Deaktivieren der Zwei-Faktor-Authentifizierung wird nicht unterstützt. Dieses Szenario enthält Schritte zum Konfigurieren der zweistufigen Authentifizierung bei der ersten Anmeldung und zum Konfigurieren der Einstellungen für die Zwei-Faktor-Authentifizierung auf dem Administrationsserver.

Schritte

Die Konfiguration der Zwei-Faktor-Authentifizierung erfolgt in mehreren Schritten:

1. **Installation einer Authenticator-App auf einem Gerät**

Sie können jede Anwendung installieren, die den Time-based One-time Password-Algorithmus (TOTP) unterstützt.

In Russland verfügbar:

- Bitrix24 OTP
- Yandex ID
- Avanpost Authenticator
- Aladdin 2FA
- Rutoken OTP

Weltweit verfügbar (einschließlich Russland):

- Google Authenticator
- Microsoft Authenticator

Um zu überprüfen, ob Kaspersky Security Center Linux die von Ihnen verwendete Authenticator-App unterstützt, aktivieren Sie die Zwei-Faktor-Authentifizierung für alle Benutzer oder für einen bestimmten Benutzer.

Einer der Schritte schlägt vor, dass Sie den Sicherheitscode angeben, der von der Authenticator-App generiert wird. Wenn dies erfolgreich ist, unterstützt Kaspersky Security Center Linux den ausgewählten Authenticator.

> Wir raten dringend davon ab, die Authenticator-App auf demselben Gerät zu installieren, von dem aus der Administrationsserver verwaltet wird.

2. **Synchronisieren Sie die Uhrzeit auf dem Gerät mit der Authenticator-App mit der Uhrzeit des Geräts, auf dem der Administrationsserver installiert ist**

   Stellen Sie sicher, dass die Uhrzeit auf dem Gerät mit der Authenticator-App und die Uhrzeit auf dem Gerät mit dem Administrationsserver mit der UTC-Zeit synchronisiert sind. Für eine höhere Genauigkeit empfehlen wir, in Ihrer gesamten Infrastruktur dieselben NTP-Server zu verwenden. Andernfalls können bei der Konfiguration der Zwei-Faktor-Authentifizierung Fehler auftreten.

3. **Konfigurieren Sie die Zwei-Faktor-Authentifizierung für Benutzerkonten bei der Anmeldung an der Web Console**

   Melden Sie sich an der Web Console an und konfigurieren Sie die Zwei-Faktor-Authentifizierung.

   Wenn Ihnen die Konfiguration der Zwei-Faktor-Authentifizierung nicht zur Verfügung steht, wenden Sie sich an einen Benutzer, der über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** verfügt und konfigurierte Zwei-Faktor-Authentifizierung hat, um Ihr Konto zur Allow-Liste für Zwei-Faktor-Authentifizierung hinzuzufügen.

4. **Konfigurieren Sie die Einstellungen für die Zwei-Faktor-Authentifizierung auf dem Administrationsserver**

   Wenn Sie die Zwei-Faktor-Authentifizierung konfiguriert haben und die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** konfiguriert haben, können Sie die Einstellungen für die Zwei-Faktor-Authentifizierung auf dem Administrationsserver wie folgt konfigurieren:

   1. Überprüfen Sie die Liste der Benutzer, die die zweistufige Authentifizierung bei der Anmeldung konfigurieren

können:

- Zur Installation von Administration Server 16.1 von Grund auf: Fügen Sie die erforderlichen Benutzer zur Allow-Liste für Zwei-Faktor-Authentifizierung damit sie Zwei-Faktor-Authentifizierung konfigurieren bei seinem oder ihrem ersten Anmeldung.
- Für ein Upgrade oder eine Wiederherstellung auf Administration Server 16.1: Überprüfen Sie die Allow-Liste für die Zwei-Faktor-Authentifizierung und löschen Sie Konten, die keinen Zugriff auf den Administrationsserver haben dürfen.

2. Benutzerkonten ausschließen, für die Sie keine Zwei-Faktor-Authentifizierung aktivieren müssen (optional)

   Bei Bedarf können Sie Benutzerkonten von der Zwei-Faktor-Authentifizierung ausschließen damit sie sich auch dann beim Administrationsserver anmelden können, wenn sie keine Zwei-Faktor-Authentifizierung konfiguriert haben. Das Ausschließen von Benutzerkonten von der Zwei-Faktor-Authentifizierung kann für Integrationskonten erforderlich sein, die während der Authentifikation keinen Sicherheitscode verwenden können. Integrationskonten werden verwendet, um Skripte über OpenAPI auszuführen.

3. Zurücksetzen oder Löschen eines geheimen Schlüssels für die Zwei-Faktor-Authentifizierung (optional)

   Sie können einen geheimen Schlüssel für die Zwei-Faktor-Authentifizierung zurücksetzen, wenn ein Benutzer den Zugriff auf sein Zwei-Faktor-Authentifizierungsgerät verliert oder die Zwei-Faktor-Authentifizierung auf einem neuen Gerät einrichten muss. Sie können auch einen geheimen Schlüssel für Ihr eigenes Konto zurücksetzen.

   Sie können einen geheimen Schlüssel löschen, um einen Benutzer vollständig daran zu hindern, sich bei der Web Console anzumelden, und um zu verhindern, dass der Benutzer auf den Administrationsserver zugreift.

4. Bearbeiten des Namens eines Sicherheitscode-Ausstellers (optional)

   Wenn Sie mehrere Administrationsserver mit ähnlichen Namen haben, müssen Sie möglicherweise die Namen der Sicherheitscode-Aussteller ändern, damit verschiedene Administrationsserver besser erkannt werden.

Ergebnisse

Nach Abschluss dieses Szenarios:

- Die Zwei-Faktor-Authentifizierung wird für Ihr eigenes Konto und für ein anderes Benutzerkonto konfiguriert, das Zugriff auf den Administrationsserver benötigt.
- Integrationskonten sind von der Zwei-Faktor-Authentifizierung ausgeschlossen.

Über die Zwei-Faktor-Authentifizierung für ein Benutzerkonto

Benutzern der Kaspersky Security Center Web Console stellt Kaspersky Security Center Linux eine Zwei-Faktor-Authentifizierung zur Verfügung. Die Zwei-Faktor-Authentifizierung basiert auf dem Standard RFC 6238 (TOTP: Time-based One-time Password-Algorithmus).

Jedes Mal, wenn Sie sich bei der Kaspersky Security Center Web Console anmelden, geben Sie Ihren Benutzernamen, Ihr Passwort und einen zusätzlichen Einmal-Sicherheitscode ein. Um einen Einmal-Sicherheitscode zu erhalten, müssen Sie eine Authenticator-App auf Ihrem Mobilgerät oder Computer installiert haben.

Jede Authentifizierungssoftware, die den Time-based One-time Password-Algorithmus (TOTP) unterstützt, ist als Authenticator-App geeignet, z. B. der Google Authenticator. Um den Einmal-Sicherheitscode zu generieren, müssen Sie die auf dem Gerät mit der Authenticator-App eingestellte Uhrzeit mit der auf dem Administrationsserver-Gerät eingestellten Uhrzeit synchronisieren. Für eine höhere Genauigkeit empfehlen wir, in Ihrer gesamten Infrastruktur dieselben NTP-Server zu verwenden.

Um zu überprüfen, ob Kaspersky Security Center Linux die von Ihnen gewünschte Authentifizierungs-App unterstützt, versuchen Sie, die Zwei-Faktor-Authentifizierung mit dieser Authentifizierungs-App zu konfigurieren.

In einem der Schritte wird empfohlen, den von der Authenticator-App generierten Einmal-Sicherheitscode anzugeben. Wenn dies erfolgreich ist, unterstützt Kaspersky Security Center Linux den ausgewählten Authenticator.

Erstellen Sie einen geheimen Code mithilfe einer Authenticator-App

Eine Authenticator-App generiert den Sicherheitscode wie folgt:

1. Der Administrationsserver erstellt einen speziellen geheimen Schlüssel sowie einen QR-Code.
2. Sie übergeben den erstellten geheimen Schlüssel oder QR-Code an die Authenticator-App.
3. Die Authenticator-App generiert einen Einmal-Sicherheitscode, den Sie an das Authentifizierungsfenster des Administrationsservers übergeben.

Ein Sicherheitscode besitzt eine Kennung, die als *Aussteller-Name* bezeichnet wird. Der Name des Sicherheitscode-Ausstellers wird als Kennung des Administrationsservers in der Authenticator-App verwendet. Sie können den Namen des Sicherheitscode-Ausstellers ändern. Der Standardwert für den Namen des Sicherheitscode-Ausstellers entspricht dem Namen des Administrationsservers. Nach der nächsten Anmeldung wird dem Administrationsserver ein neuer Name für die Ausgabe von Sicherheitscodes zugewiesen. Ein Sicherheitscode ist einmalig verwendbar und bis zu 30 Sekunden lang gültig (die genaue Zeit kann variieren).

Es wird dringend empfohlen, dass Sie den geheimen Schlüssel (oder den QR-Code) speichern und an einem sicheren Ort aufbewahren. Dies hilft Ihnen dabei, den Zugriff auf die Kaspersky Security Center Web Console wiederherzustellen, falls Sie den Zugriff auf das Gerät mit der Authenticator-App verlieren.

Die Zwei-Faktor-Authentifizierung hat folgende Eigenschaften:

- Ab der Administrationsserver-Version 16.1 ist die Zwei-Faktor-Authentifizierung automatisch aktiviert und die Option zur Konfiguration der Zwei-Faktor-Authentifizierung bei der Anmeldung ist standardmäßig deaktiviert. Die Konfiguration der Zwei-Faktor-Authentifizierung bei der Anmeldung ist nur für Benutzer verfügbar, die in der Allow-Liste für Zwei-Faktor-Authentifizierung enthalten sind.
- Ein Benutzer kann die Zwei-Faktor-Authentifizierung nur für sein eigenes Konto konfigurieren.
- Ein Benutzer kann Konten von der Zwei-Faktor-Authentifizierung ausschließen. Dies kann für Integrationskonten erforderlich sein, die keinen Einmal-Sicherheitscode zur Authentifizierung empfangen können. Integrationskonten werden verwendet, um Skripte über OpenAPI auszuführen.
- Um einen geheimen Schlüssel für die Zwei-Faktor-Authentifizierung neu zu generieren, muss ein Benutzer den geheimen Schlüssel für sein eigenes Konto zurücksetzen.

- Um einen geheimen Schlüssel für die Zwei-Faktor-Authentifizierung für das Konto eines anderen Benutzers zurückzusetzen oder zu löschen, muss ein Benutzer über ein Konto mit konfigurierter Zwei-Faktor-Authentifizierung und über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** verfügen.

- Um Konten anderer Benutzer von der Zwei-Faktor-Authentifizierung auszuschließen oder die Allow-Liste für die Zwei-Faktor-Authentifizierung zu ändern, muss ein Benutzer über ein Konto mit konfigurierter Zwei-Faktor-Authentifizierung und über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** verfügen.

- Es sollte stets mindestens ein Benutzer existieren, für den die Zwei-Faktor-Authentifizierung konfiguriert ist, damit er die Allow-Liste und Deny-Liste der Zwei-Faktor-Authentifizierung verwalten kann.

- Die Zwei-Faktor-Authentifizierung wird automatisch nur für die Administrationsserver-Version 16.1 aktiviert. Wenn andere primäre oder sekundäre Administrationsserver mit Version 16 oder früher laufen, bleiben ihre Einstellungen für die Zwei-Faktor-Authentifizierung unverändert.

- Ein virtueller Verwaltungsserver übernimmt die Einstellungen für die Zwei-Faktor-Authentifizierung vom physischen Administrationsserver, sodass die Zwei-Faktor-Authentifizierung, wenn sie auf dem physischen Administrationsserver aktiviert ist, auch auf einem virtuellen Administrationsserver aktiviert ist. Sie können die Einstellungen für die Zwei-Faktor-Authentifizierung nicht auf einem virtuellen Administrationsserver konfigurieren.

- Damit die Zwei-Faktor-Authentifizierung korrekt funktioniert, müssen Sie den Administrationsserver und die Web Console auf Version 16.1 oder höher aktualisieren.

Um einen umfassenden Schutz durch die Verwendung der Zwei-Faktor-Authentifizierung zu gewährleisten, muss nicht nur der Administrationsserver, sondern auch das Gerät, auf dem er installiert ist, gesichert werden. Um dies zu tun, betrachten Sie die Härtungsleitfaden-Empfehlungen.

Konfigurieren eines geheimen Schlüssels für die Zwei-Faktor-Authentifizierung bei der Anmeldung an der Kaspersky Security Center Web Console

Wenn Sie sich zum ersten Mal bei Kaspersky Security Center Linux 16.1 oder höher anmelden, wird das Fenster zur Konfiguration der Zwei-Faktor-Authentifizierung geöffnet.

So konfigurieren Sie die Zwei-Faktor-Authentifizierung für Ihr Benutzerkonto:

1. Installieren Sie eine beliebige Anwendung, die den Time-based One-time Password-Algorithmus (TOTP) unterstützt, auf dem Mobilgerät oder Computer, z. B.:
   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID
   - Avanpost Authenticator

- Aladdin 2FA
- Rutoken OTP

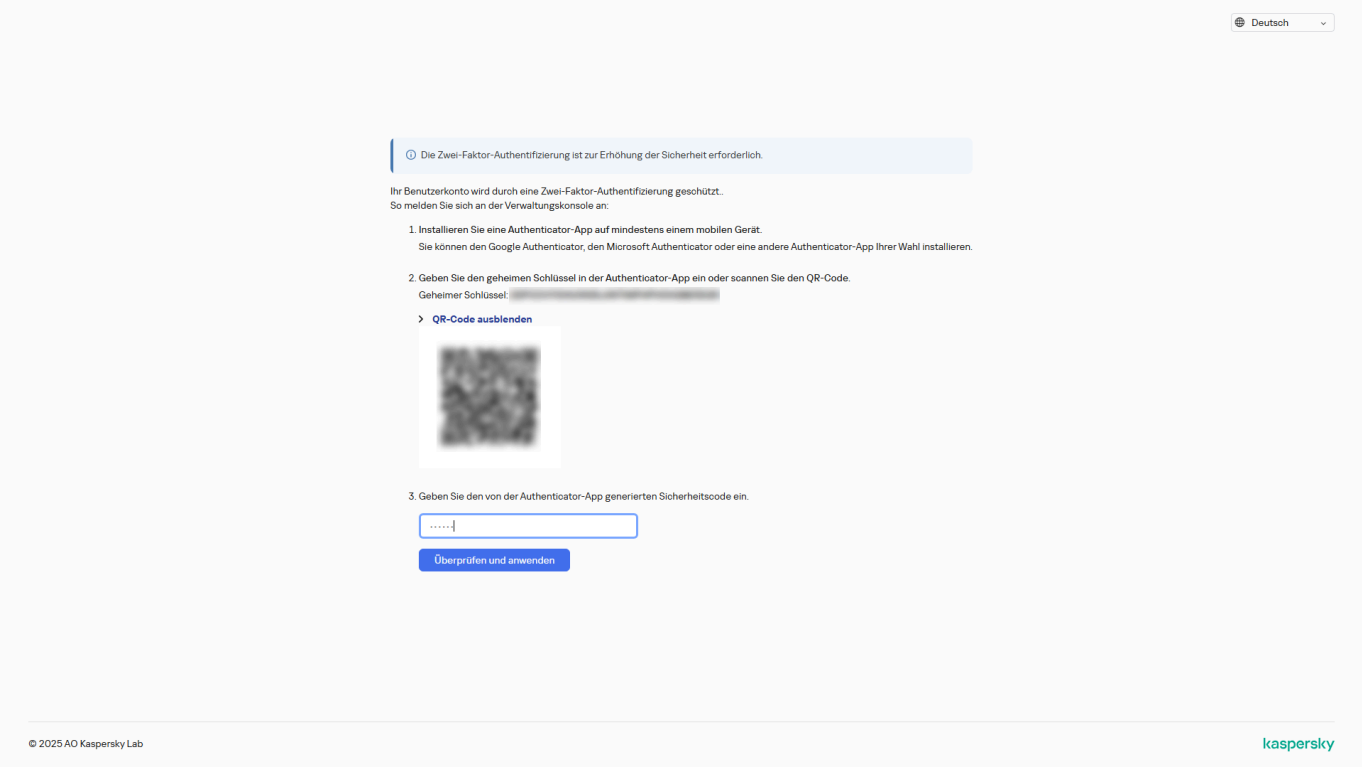
> Wir raten dringend davon ab, die Authenticator-App auf demselben Gerät zu installieren, von dem aus der Administrationsserver verwaltet wird.

2. Stellen Sie sicher, dass die Uhrzeit auf dem Gerät mit der Authenticator-App und die Uhrzeit auf dem Gerät mit dem Administrationsserver mit der UTC-Zeit synchronisiert sind. Für eine höhere Genauigkeit empfehlen wir, in Ihrer gesamten Infrastruktur dieselben NTP-Server zu verwenden.

3. Generieren Sie mithilfe der Authenticator-App auf dem mobilen Gerät oder Computer einen Einmal-Sicherheitscode. Führen Sie dazu eine der folgenden Maßnahmen durch:

   - Geben Sie den geheimen Schlüssel für die Zwei-Faktor-Authentifizierung manuell in die Authentifizierungs-App ein.
   - Klicken Sie auf **QR-Code anzeigen** und scannen Sie den QR-Code mithilfe der Authenticator-App.

   Auf dem Mobilgerät wird ein Einmal-Sicherheitscode mit 6 Ziffern angezeigt.



Konfigurieren eines geheimen Schlüssels für die Zwei-Faktor-Authentifizierung bei der Anmeldung an der Kaspersky Security Center Web Console

4. Geben Sie im Fenster der **Zwei-Faktor-Authentifizierung** den Einmal-Sicherheitscode an, der von der Authenticator-App generiert wurde, und klicken Sie anschließend auf **Überprüfen und anwenden**.

Konfiguration von Rutoken OTP

Wenn Sie Rutoken OTP verwenden, benötigen Sie ein Android-Mobilgerät mit installierter Rutoken-OTP-App. Das Android-Mobilgerät muss die folgenden Anforderungen erfüllen:

- Das Betriebssystem ist Android 7 oder höher.
- Es ist ein NFC-Modul vorhanden und aktiviert.

In der Rutoken-OTP-App müssen Sie die folgenden Parameter konfigurieren:

- Scannen Sie den QR-Code, der im Assistenten für die zweistufige Konfiguration angezeigt wird.
- Stellen Sie das Zeitintervall auf 30 Sekunden ein.
- Wählen Sie als SHA1-Algorithmus aus.

So konfigurieren Sie Rutoken OTP:

1. Legen Sie das Rutoken OTP-Gerät neben das mobile Gerät mit dem NFC-Modul.
2. Drücken Sie in der Rutoken OTP-Anwendung auf **Token verbinden**.
3. Drücken Sie in der Rutoken OTP-Anwendung auf **Einstellungen konfigurieren** und anschließend auf **Geheimen Schlüssel speichern**.

   Wenn der Token erfolgreich mit dem mobilen Gerät verbunden wurde, zeigt die Rutoken OTP-Anwendung die folgenden Statusmeldungen an:

   - **Token ist verbunden.**
   - **Einstellungen sind konfiguriert.**
   - **Geheimer Schlüssel ist gespeichert.**
4. Drücken Sie auf dem Rutoken-OTP-Gerät die Taste.

   Auf dem Gerät wird ein Sicherheitscode angezeigt.
5. Geben Sie in der Kaspersky Security Center Web Console im Fenster für die zweistufigen Überprüfung den Sicherheitscode ein.

Die Zwei-Faktor-Authentifizierung ist für Ihr Konto konfiguriert. Sie können entsprechend Ihren Rechten auf den Administrationsserver zugreifen.

Wenn Ihnen die Konfiguration der Zwei-Faktor-Authentifizierung nicht zur Verfügung steht, wenden Sie sich an einen Benutzer, der über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** verfügt und konfigurierte Zwei-Faktor-Authentifizierung hat, um Ihr Konto zur Allow-Liste für Zwei-Faktor-Authentifizierung hinzuzufügen.

Benutzern die Konfiguration der Zwei-Faktor-Authentifizierung ermöglichen

Die Allow-Liste für die Zwei-Faktor-Authentifizierung ist eine Liste von Benutzern, die berechtigt sind, die Zwei-Faktor-Authentifizierung zunächst zu konfigurieren, wenn Anmeldung bei der Web Console. Diese Liste enthält Benutzerkonten ohne konfigurierte Zwei-Faktor-Authentifizierung. Standardmäßig sind neue Benutzerkonten nicht in der Allow-Liste für die Zwei-Faktor-Authentifizierung enthalten und müssen von einem Administrator zur Liste hinzugefügt werden. Wenn es sich bei einem neuen Konto um ein Integrationskonto handelt, das zum Ausführen von OpenAPI Skripte, es muss sein von der Zwei-Faktor-Authentifizierung ausgeschlossen.

Ein Benutzerkonto wird automatisch aus der Allow-Liste für die Zwei-Faktor-Authentifizierung gelöscht, wenn für es die Zwei-Faktor-Authentifizierung konfiguriert ist oder wenn es von der Zwei-Faktor-Authentifizierung ausgeschlossen ist.

Die manuelle Änderung der Allow-Liste für die Zwei-Faktor-Authentifizierung ist für Konten verfügbar, die die Zwei-Faktor-Authentifizierung konfiguriert wurden und über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** verfügen.

So fügen Sie ein Benutzerkonto manuell zur Allow-Liste der Zwei-Faktor-Authentifizierung hinzu:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Auf der **Zwei-Faktor-Authentifizierung**-Registerkarte des Eigenschaftenfensters, in der Tabelle **Benutzer, die geheime Schlüssel erstellen dürfen**, klicken Sie auf die **Hinzufügen** Schaltfläche.

3. Führen Sie in dem neuen Fenster folgende Schritte aus:

   a. Wählen Sie das Benutzerkonto aus, das Sie hinzufügen möchten.

      Nur Benutzer, die nicht von der Zwei-Faktor-Authentifizierung ausgeschlossen sind und keinen geheimen Schlüssel für die Zwei-Faktor-Authentifizierung besitzen, können zur Allow-Liste der Zwei-Faktor-Authentifizierung hinzugefügt werden.

   b. Wenn das Konto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Geben Sie im **Schutz des Benutzerkontos**-Fenster die Anmeldeinformationen Ihres eigenen Kontos und den Einmal-Sicherheitscode für die Zwei-Faktor-Authentifizierung an.

   c. Speichern Sie die Änderungen.

   Das ausgewählte Benutzerkonto wird zur Allow-Liste für die Zwei-Faktor-Authentifizierung hinzugefügt. Bei der nächsten Anmeldung kann der Benutzer einen geheimen Schlüssel generieren.

Ein Benutzerkonto kann so lange aus der Allow-Liste für die Zwei-Faktor-Authentifizierung gelöscht werden, bis die Zwei-Faktor-Authentifizierung für dieses Konto konfiguriert ist.

So löschen Sie Benutzerkonten manuell aus der Allow-Liste für die Zwei-Faktor-Authentifizierung:

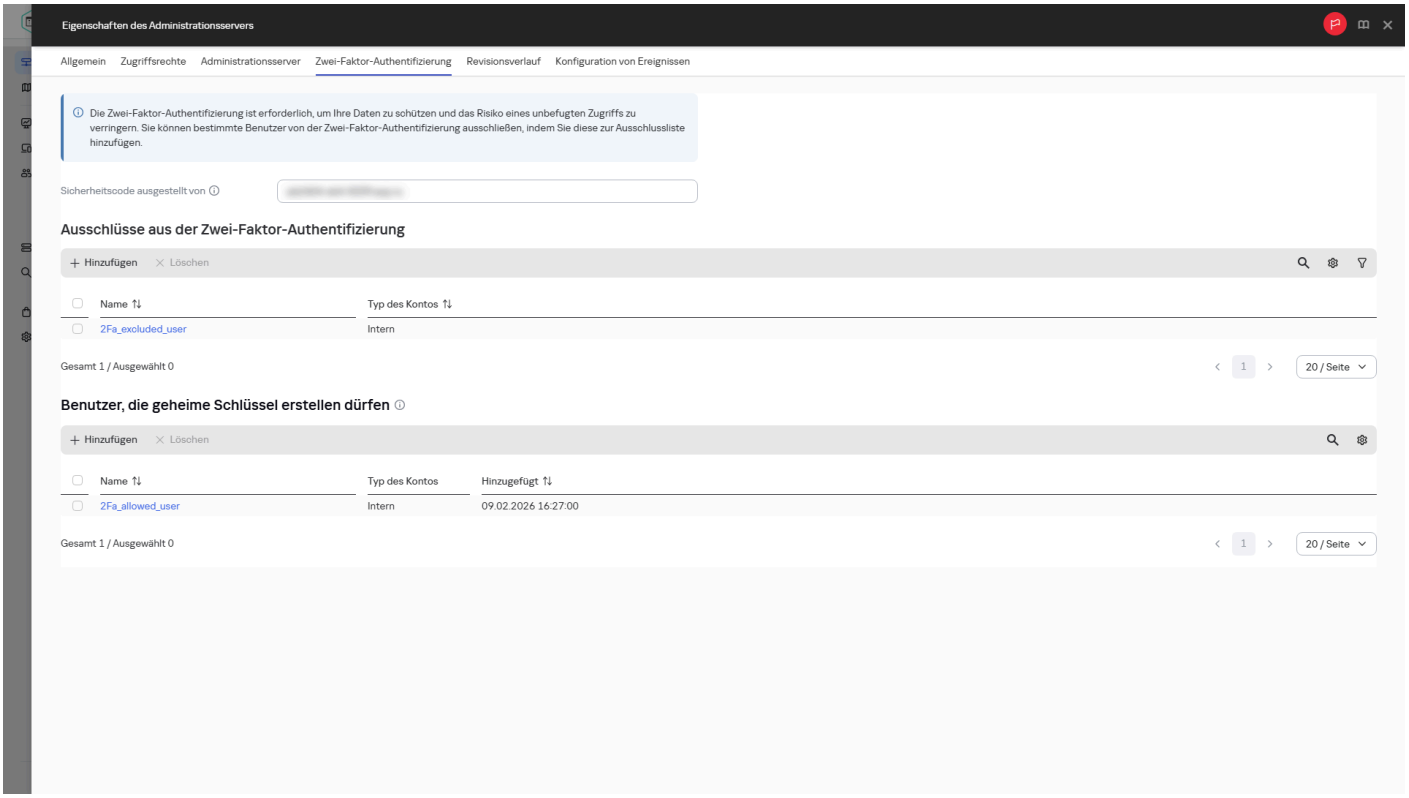
1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der **Zwei-Faktor-Authentifizierung**-Registerkarte des Eigenschaftenfensters, in der Tabelle **Benutzer, die geheime Schlüssel erstellen dürfen** die Benutzerkonten aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.

3. Wenn das Konto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Geben Sie im **Schutz des Benutzerkontos**-Fenster die Anmeldeinformationen Ihres eigenen Kontos und den Einmal-Sicherheitscode für die Zwei-Faktor-Authentifizierung an.

Die ausgewählten Benutzerkonten werden von der Allow-Liste der Zwei-Faktor-Authentifizierung gelöscht.



Allow-Liste der Zwei-Faktor-Authentifizierung konfigurieren

Wenn während einer aktiven Sitzung auf dem Administrationsserver Ihr geheimer Schlüssel für die Zwei-Faktor-Authentifizierung von einem anderen Benutzer gelöscht wird oder Sie den Schlüssel selbst zurücksetzen, aber keinen neuen erstellen, wird die Möglichkeit zum Ändern der Allow-Liste der Zwei-Faktor-Authentifizierung gesperrt.

Benutzerkonten können auch automatisch zur Allow-Liste für die Zwei-Faktor-Authentifizierung hinzugefügt und daraus gelöscht werden.

Wenn Sie einen geheimen Schlüssel für die Zwei-Faktor-Authentifizierung für andere Konten zurücksetzen, werden deren Konten automatisch zur Allow-Liste der Zwei-Faktor-Authentifizierung hinzugefügt, damit sie einen neuen geheimen Schlüssel generieren können.

Bei der Aktualisierung des Administrationsservers von Version 16 oder früher auf Version 16.1 oder später, sowie wenn Sie eine Datensicherung auf Administration Server 16 oder früher erstellen und Sie sie auf Administration Server 16.1 oder später wiederherstellen, werden Benutzerkonten automatisch zur Allow-Liste der Zwei-Faktor-Authentifizierung hinzugefügt, wenn alle folgenden Bedingungen erfüllt sind:

- Der Benutzer hat die Leseberechtigung im Funktionsbereich *Allgemeine Funktionen: Basisfunktionen* direkt dem Benutzer zugewiesen (nicht über eine Sicherheitsgruppe). Der Geltungsbereich der Benutzerrolle mit dieser Berechtigung muss alle verwalteten und nicht zugewiesenen Geräte umfassen und auf der Administrationsserver-Ebene festgelegt sein.
- Der Benutzer ist nicht von der Zwei-Faktor-Authentifizierung ausgeschlossen.
- Der Benutzer verfügt nicht über einen geheimen Schlüssel für die Zwei-Faktor-Authentifizierung.
- Die Zwei-Faktor-Authentifizierung war nicht für alle Benutzer auf dem Administrationsserver der vorherigen Version aktiviert.

Wenn eine der Bedingungen nicht erfüllt ist, wird der Benutzer nicht zur Allow-Liste der Zwei-Faktor-Authentifizierung hinzugefügt.

Nach einem Upgrade oder einer Wiederherstellung empfehlen wir sicherzustellen, dass die Allow-Liste der Zwei-Faktor-Authentifizierung nur die Benutzerkonten enthält, die Zugriff auf den Administrationsserver haben müssen. Überprüfen Sie die Allow-Liste für Zwei-Faktor-Authentifizierung und entfernen Sie alle anderen Konten daraus. Fügen Sie die zur Ausführung von Skripten über OpenAPI verwendeten Integrationskonten zur Ausschlussliste hinzu, um Skriptfehler zu vermeiden.

Wenn alle folgenden Bedingungen erfüllt sind, verlieren die Benutzerkonten nach einem Upgrade oder einer Wiederherstellung den Zugriff auf den Administrationsserver:

- Der Benutzer hat die Leseberechtigung im Funktionsbereich *Allgemeine Funktionen: Basisfunktionen* über eine Sicherheitsgruppe zugewiesen (nicht direkt dem Benutzer) oder verfügt überhaupt nicht über diese Berechtigung.
- Der Benutzer ist nicht von der Zwei-Faktor-Authentifizierung ausgeschlossen.
- Der Benutzer verfügt nicht über einen geheimen Schlüssel für die Zwei-Faktor-Authentifizierung.
- Die Zwei-Faktor-Authentifizierung war aktiviert für alle Benutzer auf dem Administrationsserver der vorherigen Version.

Diese Konten können bei Bedarf manuell zur Allow-Liste für die Zwei-Faktor-Authentifizierung hinzugefügt werden.

Zurücksetzen und Löschen eines geheimen Schlüssels für die Zwei-Faktor-Authentifizierung

Sie können einen geheimen Schlüssel zurücksetzen, wenn ein Benutzer den Zugriff auf sein Zwei-Faktor-Authentifizierungsgerät verliert oder die Zwei-Faktor-Authentifizierung auf einem neuen Gerät einrichten muss. Durch das Zurücksetzen des geheimen Schlüssels kann der Benutzer bei der Web Console erneut anmelden und einen neuen geheimen Schlüssel generieren .

> Sie können einen geheimen Schlüssel für die Zwei-Faktor-Authentifizierung für Konten anderer Benutzer nur zurücksetzen oder löschen, wenn Sie die Zwei-Faktor-Authentifizierung konfiguriert haben und über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** verfügen. Sie können auch Ihren eigenen geheimen Schlüssel neu generieren.

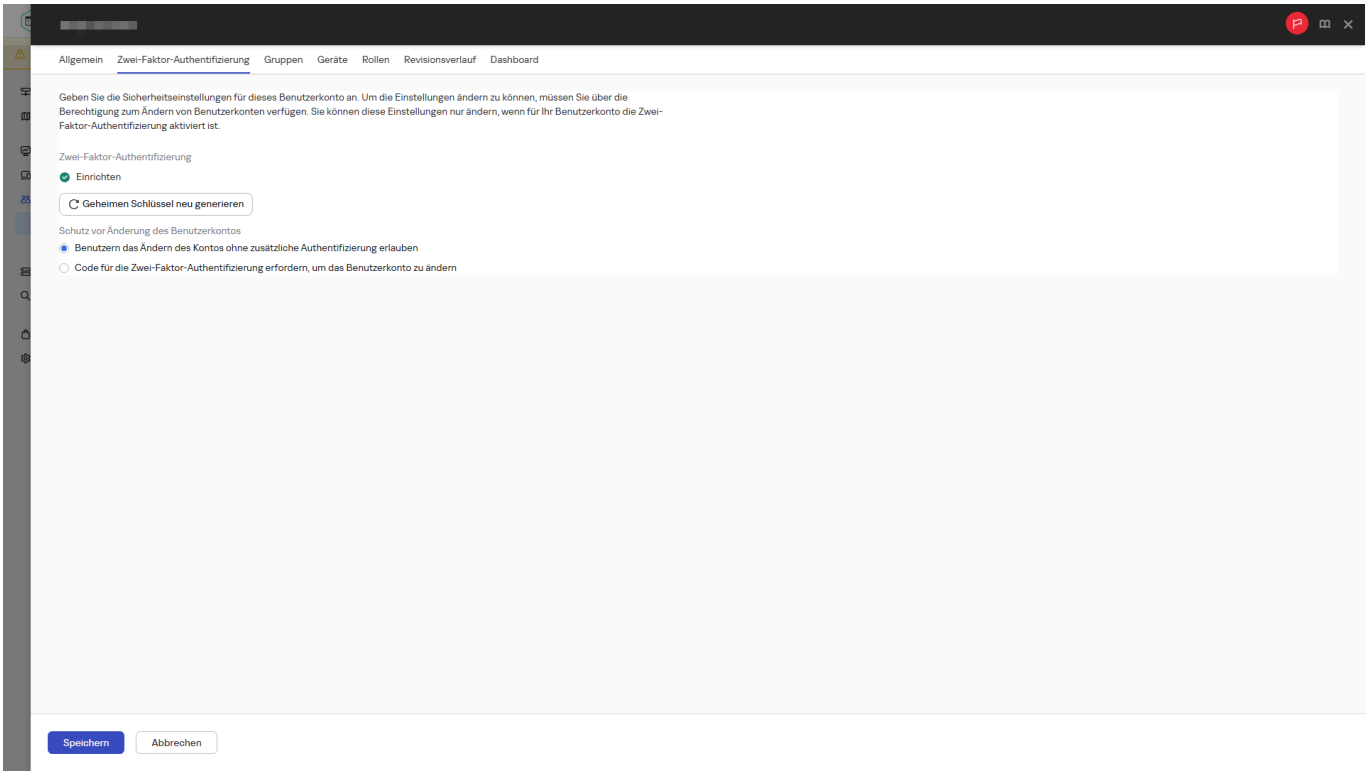
So setzen Sie einen geheimen Schlüssel für ein Konto zurück:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.

2. Klicken Sie auf den Namen des Benutzerkontos, für das Sie einen geheimen Schlüssel zurücksetzen möchten.

3. Wenn Sie einen geheimen Schlüssel für Ihr Konto zurücksetzen möchten:

   a. Auf der Registerkarte **Zwei-Faktor-Authentifizierung**, klicken Sie auf die Schaltfläche **Geheimen Schlüssel neu generieren**.

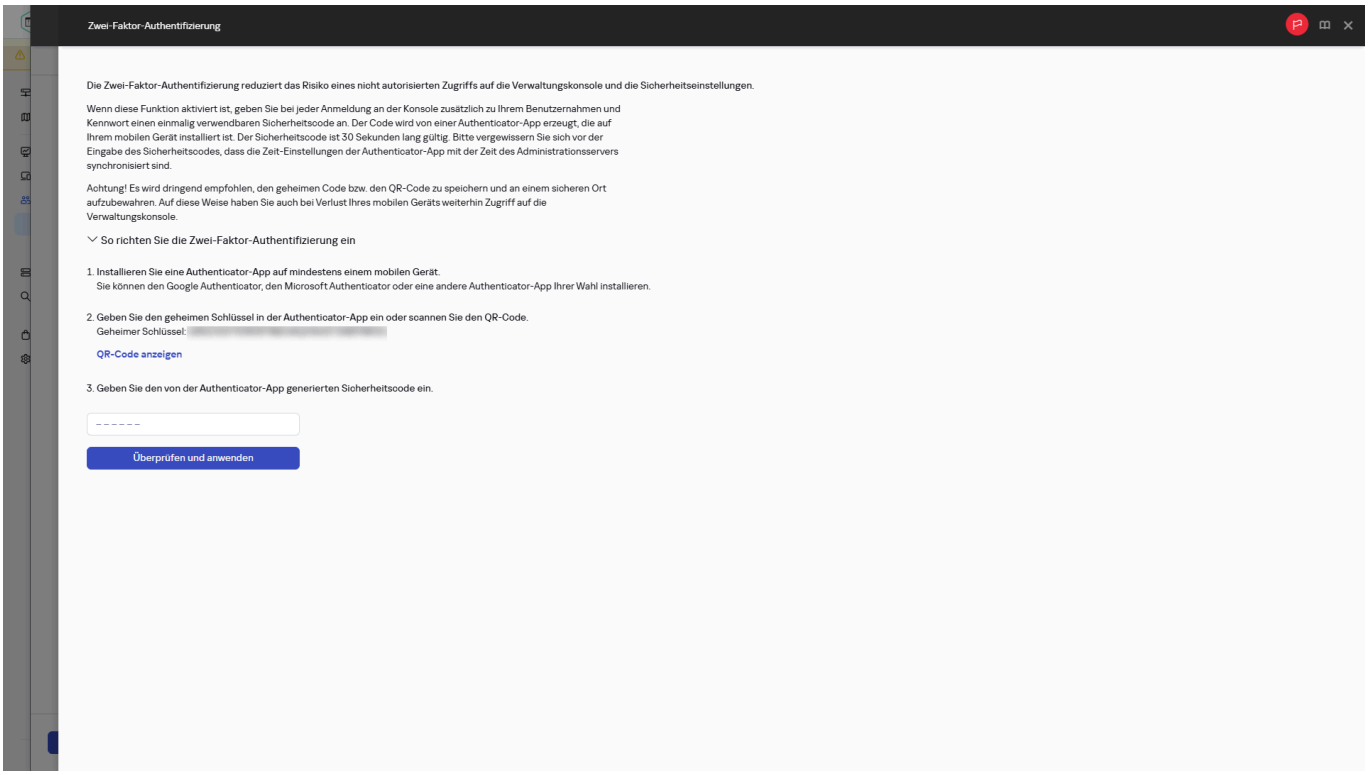


Geheimen Schlüssel der Zwei-Faktor-Authentifizierung für das aktuelle Benutzerkonto erneut generieren

   a. Wenn Ihr Konto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Geben Sie im **Schutz des Benutzerkontos**-Fenster die Anmeldedaten Ihres eigenen Kontos und den Zwei-Faktor-Authentifizierungscode an.

   b. Im **Zwei-Faktor-Authentifizierung**-Fenster, klicken Sie **So richten Sie die Zwei-Faktor-Authentifizierung ein**, und dann klicken Sie **QR-Code anzeigen**.

   c. Verwenden Sie die Authenticator-App auf Ihrem Mobilgerät, um den QR-Code zu scannen und einen Einmal-Sicherheitscode zu erhalten.



Neuen geheimen Schlüssel der Zwei-Faktor-Authentifizierung für das aktuelle Benutzerkonto generieren

a. Im **Zwei-Faktor-Authentifizierung**-Fenster, geben Sie den Einmal-Sicherheitscode ein, der von der Authenticator-App generiert wurde, klicken Sie auf die Schaltfläche **Überprüfen und anwenden** und speichern Sie anschließend die Änderungen.

Konfiguration von Rutoken OTP

Wenn Sie Rutoken OTP verwenden, benötigen Sie ein Android-Mobilgerät mit installierter Rutoken-OTP-App. Das Android-Mobilgerät muss die folgenden Anforderungen erfüllen:

- Das Betriebssystem ist Android 7 oder höher.
- Es ist ein NFC-Modul vorhanden und aktiviert.

In der Rutoken-OTP-App müssen Sie die folgenden Parameter konfigurieren:

- Scannen Sie den QR-Code, der im Assistenten für die zweistufige Konfiguration angezeigt wird.
- Stellen Sie das Zeitintervall auf 30 Sekunden ein.
- Wählen Sie als SHA1-Algorithmus aus.

So konfigurieren Sie Rutoken OTP:

1. Legen Sie das Rutoken OTP-Gerät neben das mobile Gerät mit dem NFC-Modul.
2. Drücken Sie in der Rutoken OTP-Anwendung auf **Token verbinden**.
3. Drücken Sie in der Rutoken OTP-Anwendung auf **Einstellungen konfigurieren** und anschließend auf **Geheimen Schlüssel speichern**.

Wenn der Token erfolgreich mit dem mobilen Gerät verbunden wurde, zeigt die Rutoken OTP-Anwendung die folgenden Statusmeldungen an:

- **Token ist verbunden.**
- **Einstellungen sind konfiguriert.**
- **Geheimer Schlüssel ist gespeichert.**

4. Drücken Sie auf dem Rutoken-OTP-Gerät die Taste.

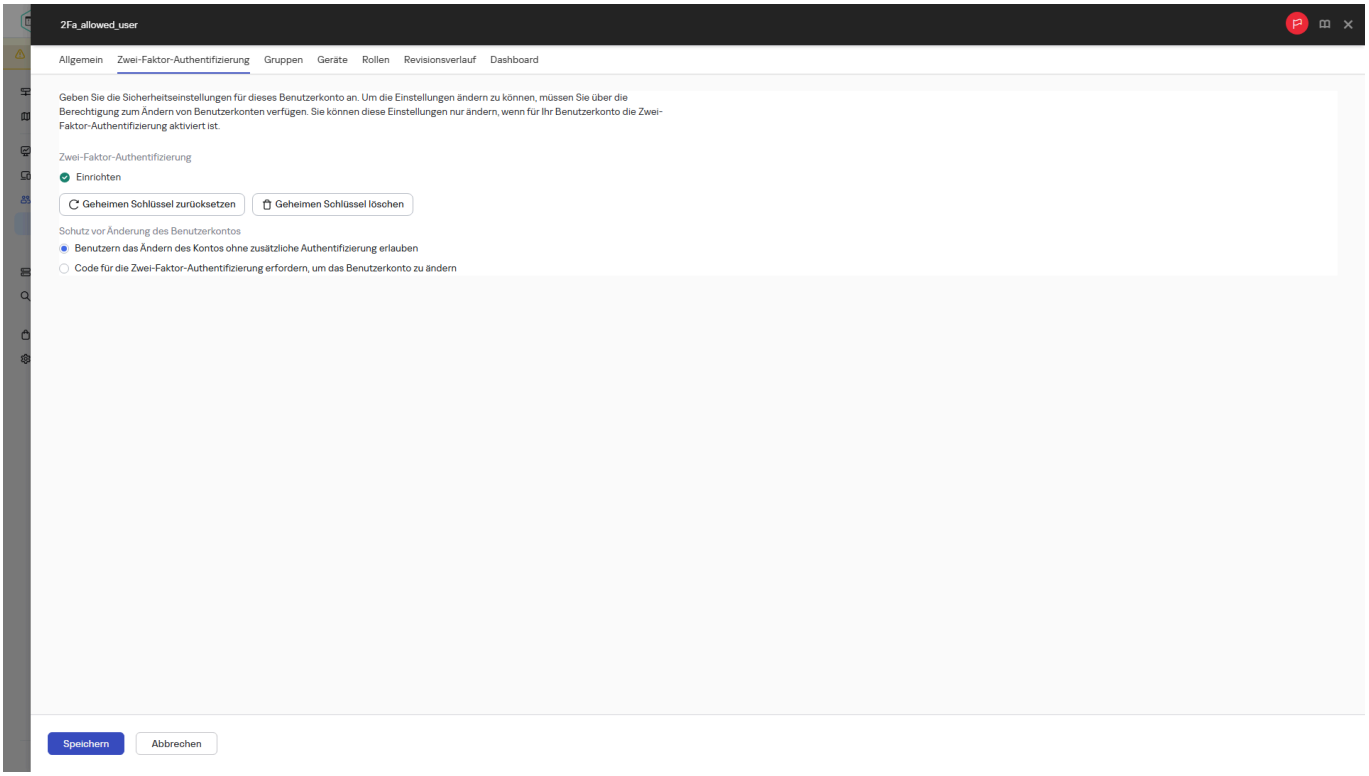
   Auf dem Gerät wird ein Sicherheitscode angezeigt.

5. Geben Sie in der Kaspersky Security Center Web Console im Fenster für die zweistufigen Überprüfung den Sicherheitscode ein.

Der geheime Schlüssel für Ihr Konto wurde geändert.

4. Wenn Sie einen geheimen Schlüssel für ein anderes Konto zurücksetzen möchten:

   a. Auf der **Zwei-Faktor-Authentifizierung**-Registerkarte, klicken Sie auf die Schaltfläche **Geheimen Schlüssel zurücksetzen**.



Geheimen Schlüssel der Zwei-Faktor-Authentifizierung für ein anderes Benutzerkonto zurücksetzen

   a. Wenn das Konto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Im **Schutz des Benutzerkontos**-Fenster die Anmeldedaten Ihres eigenen Kontos und den Einmal-Sicherheitscode für die Zwei-Faktor-Authentifizierung an.

   b. Bestätigen Sie das Zurücksetzen des geheimen Schlüssels und speichern Sie anschließend die Änderungen.

Wenn Sie einen geheimen Schlüssel für ein anderes Konto zurücksetzen, wird der vorhandene geheime Schlüssel gelöscht und das Benutzerkonto in den Eigenschaften des Administrationsservers zur Allow-Liste der Zwei-Faktor-Authentifizierung hinzugefügt. Bei der nächsten Anmeldung kann der Benutzer einen neuen geheimen Schlüssel generieren.

Der geheime Schlüssel eines Benutzerkontos wird zurückgesetzt.

Sie können einen geheimen Schlüssel löschen, um einen Benutzer vollständig daran zu hindern, sich bei der Web Console anzumelden, und um zu verhindern, dass der Benutzer auf den Administrationsserver zugreift.

So löschen Sie einen geheimen Schlüssel:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Klicken Sie auf den Namen des internen Benutzerkontos, für das Sie einen geheimen Schlüssel löschen möchten.

   Sie können einen geheimen Schlüssel für Ihr eigenes Konto nicht löschen.

3. Auf der **Zwei-Faktor-Authentifizierung**-Registerkarte, klicken Sie auf die Schaltfläche **Geheimen Schlüssel löschen**.
4. Wenn das Konto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Im **Schutz des Benutzerkontos**-Fenster die Anmeldedaten Ihres eigenen Kontos und den Einmal-Sicherheitscode für die Zwei-Faktor-Authentifizierung an.
5. Bestätigen Sie das Löschen des geheimen Schlüssels und speichern Sie anschließend die Änderungen.

   Der geheime Schlüssel eines Benutzerkontos wird gelöscht.

Sie können den Zugriff wiederherstellen, indem Sie den Benutzer zur Allow-Liste für Zwei-Faktor-Authentifizierung in den Eigenschaften des Administrationsservers hinzufügen. In diesem Fall kann der Benutzer bei der nächsten Anmeldung einen neuen geheimen Schlüssel generieren.

Benutzerkonten von der Zwei-Faktor-Authentifizierung ausschließen

Sie können Benutzerkonten von der Zwei-Faktor-Authentifizierung ausschließen, damit sie sich auch dann beim Administrationsserver anmelden können, wenn sie keine Zwei-Faktor-Authentifizierung konfiguriert haben. Das Ausschließen von Konten von der Zwei-Faktor-Authentifizierung kann für Integrationskonten erforderlich sein, die während der Authentifizierung keinen Einmal-Sicherheitscode bereitstellen können. Integrationskonten werden verwendet, um Skripte über OpenAPI auszuführen.

Sie können die Ausschlussliste ändern, wenn für Ihr Konto die Zwei-Faktor-Authentifizierung konfiguriert ist und Sie über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** verfügen.

So schließen Sie ein Benutzerkonto von der Zwei-Faktor-Authentifizierung aus:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Auf der **Zwei-Faktor-Authentifizierung**-Registerkarte des Eigenschaftenfensters in der Tabelle **Ausschlüsse aus der Zwei-Faktor-Authentifizierung**, klicken Sie auf die **Hinzufügen**-Schaltfläche.

3. Führen Sie in dem neuen Fenster folgende Schritte aus:

   a. Wählen Sie das Benutzerkonto aus, das Sie ausschließen möchten.

   b. Wenn das Konto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Geben Sie im **Schutz des Benutzerkontos**-Fenster die Anmeldeinformationen Ihres eigenen Kontos und den Einmal-Sicherheitscode für die Zwei-Faktor-Authentifizierung an.

   c. Speichern Sie die Änderungen.

   Die ausgewählten Benutzerkonten werden von der Zwei-Faktor-Authentifizierung ausgeschlossen, und ihre geheimen Schlüssel werden gelöscht, sofern vorhanden. Die Liste der ausgeschlossenen Konten wird nicht geändert, wenn Sie Sicherung wiederherstellen auf dem Administrationsserver 16.1 oder Administrationsserver aktualisieren auf Version 16.1 oder höher. Wenn die Konten aus der Ausschlussliste in der vorherigen Version des Administrationsservers Geheimnisse enthielten, werden diese geheimen Schlüssel in 16.1 gelöscht.

Sie können Benutzerkonten aus der Ausschlussliste löschen, um Benutzern die Anmeldung bei der Web Console vollständig zu verweigern und zu verhindern, dass Benutzer auf den Administrationsserver zugreifen.

So löschen Sie Benutzerkonten aus der Ausschlussliste:

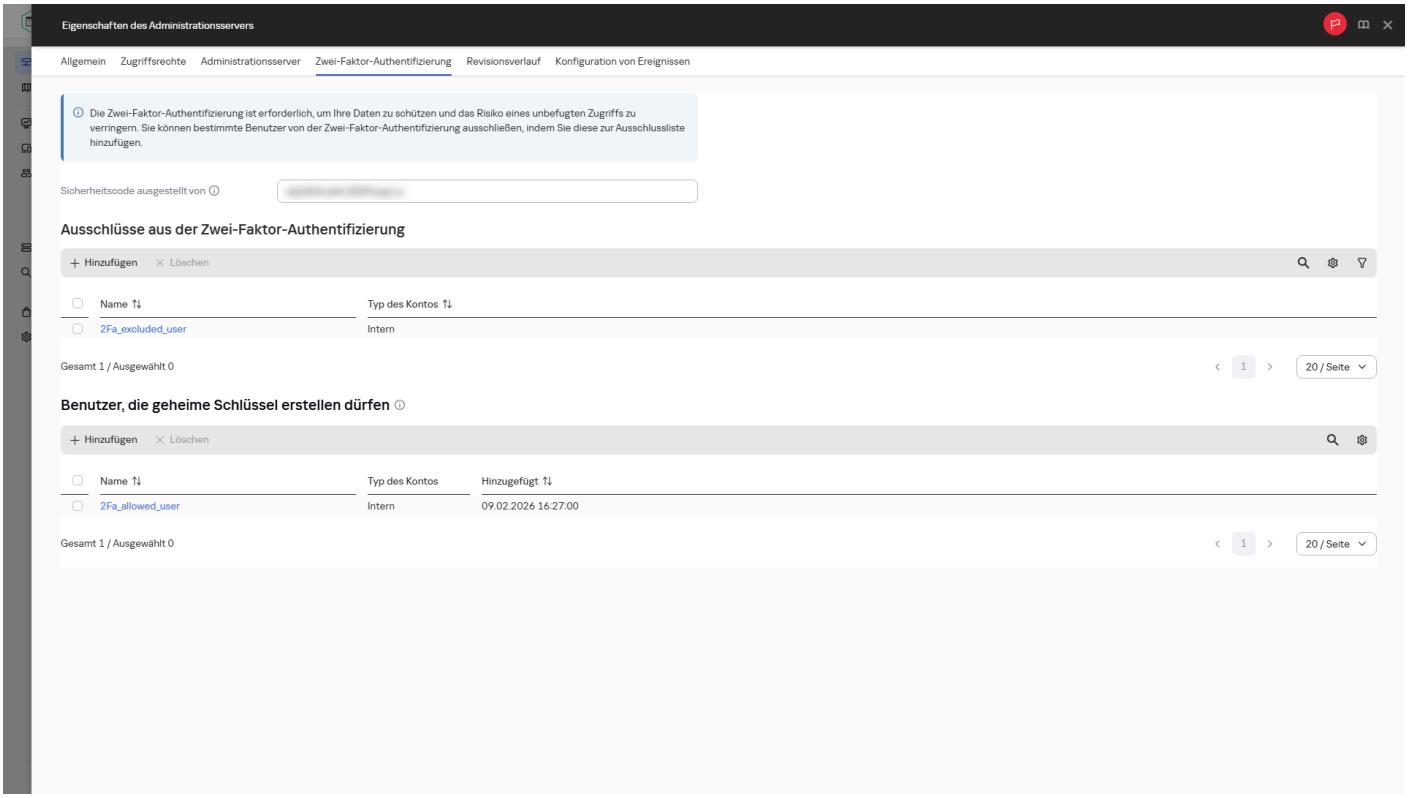
1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Auf der **Zwei-Faktor-Authentifizierung**-Registerkarte des Eigenschaftenfensters, in der Tabelle **Ausschlüsse aus der Zwei-Faktor-Authentifizierung**, wählen Sie die Benutzerkonten aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.

3. Wenn das Konto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Geben Sie im **Schutz des Benutzerkontos**-Fenster die Anmeldeinformationen Ihres eigenen Kontos und den Einmal-Sicherheitscode für die Zwei-Faktor-Authentifizierung an.

Die ausgewählten Benutzerkonten werden aus der Ausschlussliste gelöscht.



Deny-Liste der Zwei-Faktor-Authentifizierung konfigurieren

Name eines Sicherheitscode-Ausstellers bearbeiten

Sie können mehrere Identifikatoren (sogenannte Aussteller) für verschiedene Administrationsserver haben. Sie können den Namen eines Sicherheitscode-Ausstellers ändern, beispielsweise wenn der Administrationsserver bereits einen ähnlichen Namen eines Sicherheitscode-Ausstellers für einen anderen Administrationsserver verwendet. Standardmäßig entspricht der Name eines Sicherheitscode-Ausstellers dem Namen des Administrationsservers.

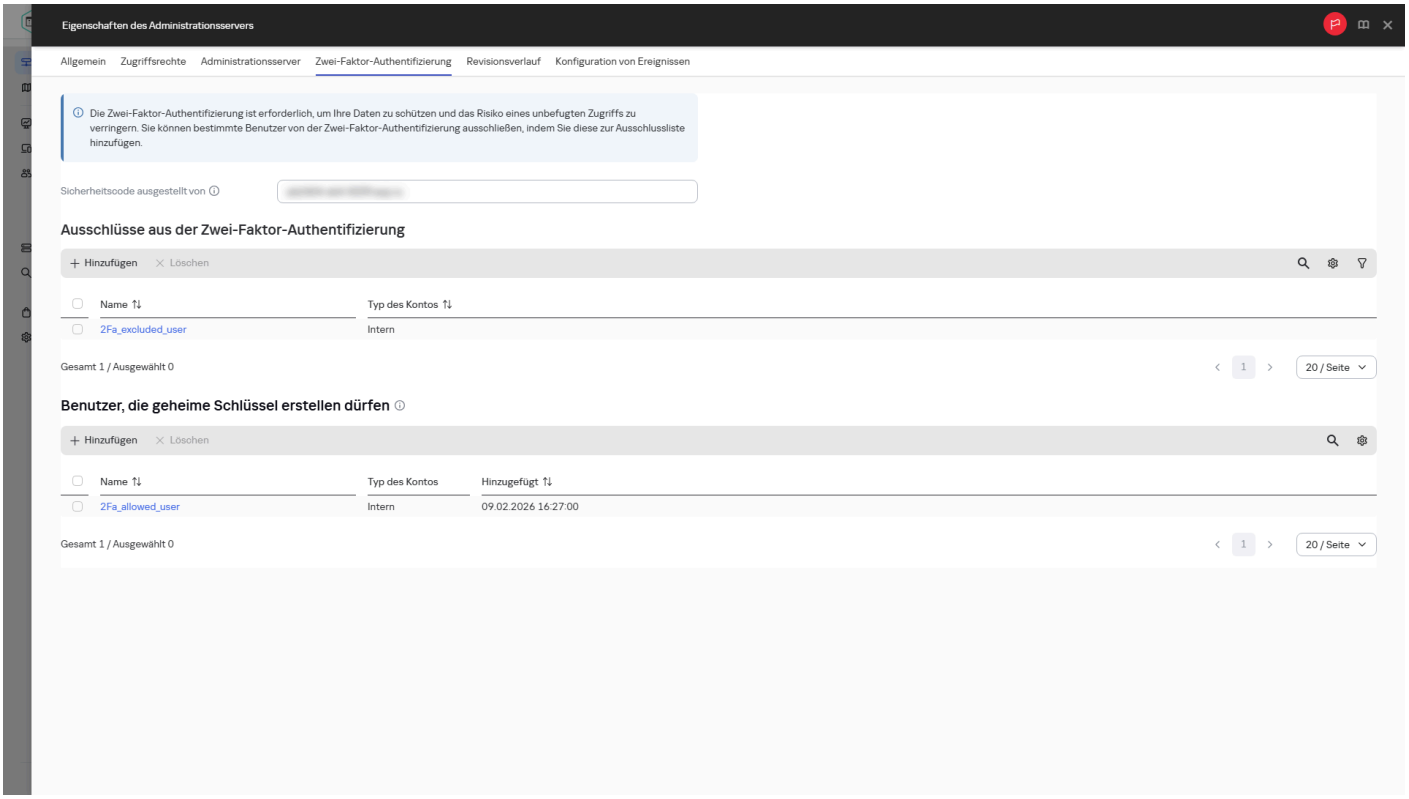
Um einen neuen Namen für einen Sicherheitscode-Aussteller anzugeben:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Geben Sie auf der Registerkarte **Zwei-Faktor-Authentifizierung** des Eigenschaftenfensters einen neuen Namen in das Feld **Sicherheitscode ausgestellt von** und speichern Sie anschließend die Änderungen.

Nach der nächsten Anmeldung wird dem Administrationsserver ein neuer Name für den Herausgeber des Sicherheitscodes zugewiesen.



Namen eines Sicherheitscode-Ausstellers angeben

Anzahl der zulässigen Eingabeversuche des Kennworts anpassen

Die Benutzer von Kaspersky Security Center Linux haben nur eine begrenzte Anzahl von Eingabeversuchen mit ungültigen Kennwörtern. Wenn das Limit erreicht ist, wird das Benutzerkonto für eine Stunde gesperrt.

Standardmäßig liegt die maximale Anzahl zulässiger Versuche zur Eingabe eines Kennworts bei 10. Sie können die Anzahl der zulässigen Kennworteingabeversuche ändern (siehe Beschreibung in diesem Abschnitt).

So ändern Sie die Anzahl der zulässigen Kennworteingabeversuche:

1. Führen Sie auf dem Administrationsserver-Gerät eine Linux-Befehlszeile aus.

2. Führen Sie für das Dienstprogramm klscflag den folgenden Befehl aus:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

Dabei steht N für die Anzahl der zulässigen Kennworteingabeversuche.

3. Um die Änderungen zu übernehmen, starten Sie den Administrationsserver-Dienst neu.

Die maximale Anzahl der Eingabeversuche für das Kennwort wird geändert.

Löschen eines Benutzers oder einer Sicherheitsgruppe

Sie können nur interne Benutzer oder interne Sicherheitsgruppen löschen.

So löschen Sie einen Benutzer oder eine Sicherheitsgruppe:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** oder **Gruppen** aus.

2. Aktivieren Sie das Kontrollkästchen neben dem Benutzer oder neben der Sicherheitsgruppe, den oder die Sie entfernen möchten.

   Es sollte stets mindestens ein Benutzer existieren, für den die Zwei-Faktor-Authentifizierung konfiguriert ist, damit er die Allow-Liste und Deny-Liste der Zwei-Faktor-Authentifizierung verwalten kann.

3. Klicken Sie auf die Schaltfläche **Löschen**.

4. Klicken Sie im folgenden Fenster auf **OK**.

Der Benutzer oder die Sicherheitsgruppe ist gelöscht.

Kennwort eines Benutzerkontos ändern

Sie müssen möglicherweise das Kennwort für Ihr eigenes Konto oder für andere Benutzerkonten ändern, wenn das aktuelle Kennwort bald abläuft oder Sie es durch ein sichereres Kennwort ersetzen möchten.

Das Kennwort muss den folgenden Regeln entsprechen:

- Das Kennwort muss zwischen 8 und 256 Zeichen lang sein.
- Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Kategorien enthalten:
  - Großbuchstaben (A–Z)
  - Kleinbuchstaben (a–z)

- Ziffern (0–9)
- Sonderzeichen (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- In einem Kennwort sind unzulässig: Leerzeichen, Unicode-Zeichen oder die Kombination von "." und "@", falls "." vor "@" steht.

Kennwort des eigenen Benutzerkontos ändern

So ändern Sie das Kennwort für Ihr Benutzerkonto:

1. Wechseln Sie im oberen Bereich zum Menü Ihres Benutzerkontos, indem Sie auf Ihren Kontonamen klicken.
2. Wählen Sie in der Dropdown-Liste die Option **Kennwort ändern** aus.
3. Geben Sie im neuen rechten Bereich das aktuelle Kennwort ein und geben Sie anschließend das neue Kennwort für die Verbindung mit Kaspersky Security Center Linux an.

   Um das eingegebene Kennwort anzuzeigen, klicken Sie auf .
4. Wenn Ihr Konto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Geben Sie im **Schutz des Benutzerkontos**-Fenster die Anmeldeinformationen Ihres eigenen Benutzerkontos oder eines Kontos an an, das über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** verfügt.
5. Geben Sie den Einmal-Sicherheitscode an, der von der Authenticator-App auf dem Mobilgerät generiert wird.

Kennwort eines internen Benutzerkontos ändern

So ändern Sie das Kennwort eines internen Benutzerkontos:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Klicken Sie auf den Namen des Benutzerkontos, das Sie bearbeiten möchten.
3. Klicken Sie im folgenden Fenster mit den Benutzereinstellungen auf der Registerkarte **Allgemein** auf die Schaltfläche **Kennwort ändern**.
4. Geben Sie ein neues Kennwort an, das für die Verbindung des Benutzers mit Kaspersky Security Center Linux verwendet wird.

   Um das eingegebene Kennwort anzuzeigen, klicken Sie auf .
5. Bei Bedarf können Sie die Option **Benutzer muss bei Erstanmeldung sein Kennwort ändern** aktivieren, um bei der nächsten Authentifizierung eines Benutzers eine Kennwortänderung zu erzwingen.
6. Wenn das Benutzerkonto gegen unbefugte Änderungen geschützt ist, müssen Sie zunächst bestätigen, dass Sie zur Kontoänderung berechtigt sind. Geben Sie im **Schutz des Benutzerkontos**-Fenster die Anmeldedaten des Kontos an, das über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen**: **Benutzerberechtigungen** verfügt.
7. Geben Sie den Einmal-Sicherheitscode an, der von der Authenticator-App auf dem Mobilgerät generiert wird.

Optionen zur Kennwortänderung mithilfe von Server-Flags konfigurieren

Sie können das Tool "klscflag" verwenden, um die Kennwortänderung mit den folgenden Befehlen zu konfigurieren:

- Konfiguration des Zeitraums für die Kennwort-Rotation (Flag `LP_SplPwdChangePeriodDays`)

  ```
  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <Rotationszeitraum>
  ```

  Wobei `<Rotationszeitraum>` für die Zeitspanne in Tagen steht, nach der das Benutzerkennwort abläuft. Mögliche Werte: 0 – 730. Wenn der Parameter den Wert "0" besitzt, ist die Rotation des Kennworts deaktiviert.

- Konfigurieren der Zeitspanne für die vorherige Warnung über eine erforderliche Kennwortänderung (Flag `LP_SplPwdChangeNotificationHours`)

  ```
  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <Warnungszeitraum>
  ```

  Wobei `<Warnungszeitraum>` für die Zeitspanne in Stunden steht, bevor das Benutzerkennwort abläuft. Während dieser Zeitspanne wird eine Benachrichtigung über die erforderliche Kennwortänderung angezeigt. Mögliche Werte: 0 – 17520. Wenn der Parameter den Wert "0" besitzt, beträgt der Warnungszeitraum 25 Prozent des Zeitraums für die Kennwort-Rotation.

- Festlegen des Standardwerts für die Option **Benutzer muss bei Erstanmeldung sein Kennwort ändern** (Flag `LP_SplPwdForceChange`)

  ```
  klscflag -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <Wert>
  ```

  Mögliche Werte des Flags `<Wert>`:

  `1` – die Option **Benutzer muss bei Erstanmeldung sein Kennwort ändern** ist aktiviert.

  `0` – Die Option **Benutzer muss bei Erstanmeldung sein Kennwort ändern** ist deaktiviert.

Um den aktuellen Wert eines Flags anzuzeigen, führen Sie den folgenden Befehl aus:

```
klscflag -fget -pv .core/.independent -s KLLIM -n <Flag> -t d
```

Wobei `<Flag>` dem Flag `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` oder `LP_SplPwdForceChange` entspricht.

Benutzerrollen erstellen

So erstellen Sie eine Benutzerrolle:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
3. Geben Sie im folgenden Fenster **Neuer Rollenname** den Namen der neuen Rolle ein.
4. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu übernehmen.
5. Ändern Sie im folgenden Fenster für Rolleneigenschaften die Einstellungen der Rolle:

   - Bearbeiten Sie auf der Registerkarte **Allgemein** den Rollennamen.

     Sie können den Namen einer vordefinierten Rolle nicht bearbeiten.

- Bearbeiten Sie auf der Registerkarte **Einstellungen** den Rollenbereich und die mit der Rolle verknüpften Richtlinien und Profile.
- Bearbeiten Sie auf der Registerkarte **Zugriffsrechte** die Berechtigungen für den Zugriff auf die Kaspersky-Anwendungen.

6. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die neue Rolle wird in der Liste der Benutzerrollen angezeigt.

Benutzerrollen bearbeiten

So bearbeiten Sie eine Benutzerrolle:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.
2. Klicken Sie auf den Namen der Rolle, die Sie bearbeiten möchten.
3. Ändern Sie im folgenden Fenster für Rolleneigenschaften die Einstellungen der Rolle:
   - Bearbeiten Sie auf der Registerkarte **Allgemein** den Rollennamen.

     Sie können den Namen einer vordefinierten Rolle nicht bearbeiten.
   - Bearbeiten Sie auf der Registerkarte **Einstellungen** den Rollenbereich und die mit der Rolle verknüpften Richtlinien und Profile.
   - Bearbeiten Sie auf der Registerkarte **Zugriffsrechte** die Berechtigungen für den Zugriff auf die Kaspersky-Anwendungen.
4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die aktualisierte Rolle wird in der Liste der Benutzerrollen angezeigt.

Gültigkeitsbereich einer Benutzerrolle bearbeiten

Ein *Benutzerrollenbereich* ist eine Kombination von Benutzern und Administrationsgruppen. Einstellungen, die mit einer Benutzerrolle verbunden sind, gelten nur für Geräte, die Benutzern gehören, die über diese Rolle verfügen, und nur, wenn diese Geräte zu Gruppen gehören, die mit dieser Rolle verbunden sind, einschließlich untergeordnete Gruppen.

Um Benutzer, Sicherheitsgruppen und Administrationsgruppen zum Bereich einer Benutzerrolle hinzuzufügen, können Sie eine der folgenden Methoden anwenden:

Methode 1:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** oder **Gruppen** aus.

2. Aktivieren Sie die Kontrollkästchen neben den Benutzern oder Sicherheitsgruppen, die Sie dem Bereich der Benutzerrolle hinzufügen möchten.

3. Klicken Sie auf die Schaltfläche **Rolle zuordnen**.

   Der Assistent zum Zuweisen einer Rolle wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

4. Wählen Sie im Schritt **Rolle auswählen** des Assistenten die Benutzerrolle aus, die Sie zuweisen möchten.

5. Wählen Sie in dem Schritt **Bereich definieren** die Administrationsgruppe aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.

6. Klicken Sie auf die Schaltfläche **Rolle zuordnen**, um das Fenster zu schließen.

Die ausgewählten Benutzer oder Sicherheitsgruppen und die ausgewählte Administrationsgruppe werden dem Bereich der Benutzerrolle hinzugefügt.

Methode 2:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.

2. Klicken Sie auf den Namen der Rolle, für die Sie den Bereich definieren möchten.

3. Wählen Sie im folgenden Eigenschaftenfenster der Rolle die Registerkarte **Einstellungen** aus.

4. Klicken Sie im Abschnitt **Bereich der Rolle** auf **Hinzufügen**.

   Der Assistent zum Zuweisen einer Rolle wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

5. Wählen Sie im Schritt **Bereich definieren** die Administrationsgruppe aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.

6. Wählen Sie im Schritt **Benutzer auswählen** die Benutzer und Sicherheitsgruppen aus, die Sie dem Gültigkeitsbereich der Benutzerrolle hinzufügen möchten.

7. Klicken Sie auf die Schaltfläche **Rolle zuordnen**, um das Fenster zu schließen.

8. Klicken Sie auf die Schaltfläche **Schließen** (⨯), um das Eigenschaftenfenster der Rolle zu schließen.

Die ausgewählten Benutzer oder Sicherheitsgruppen und die ausgewählte Administrationsgruppe werden dem Bereich der Benutzerrolle hinzugefügt.

Methode 3:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Zugriffsrechte** das Kontrollkästchen neben dem Namen des Benutzers oder der Sicherheitsgruppe, die Sie dem Benutzerrollenbereich hinzufügen möchten, und klicken Sie dann auf die Schaltfläche **Rollen**.

   Sie können nur einzelne Benutzer oder Sicherheitsgruppen auswählen. Wenn Sie mehr als ein Element auswählen, wird die Schaltfläche **Rollen** deaktiviert.

3. Wählen Sie im Fenster **Rollen** die Benutzerrolle aus, die Sie zuweisen möchten, wenden Sie dann die Änderungen an und speichern Sie sie.

   Die ausgewählten Benutzer oder Sicherheitsgruppen werden in den Geltungsbereich der Benutzerrolle aufgenommen.

Benutzerrollen löschen

So löschen Sie eine Benutzerrolle:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.
2. Aktivieren Sie die Kontrollkästchen neben dem Namen, den Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **OK**.

Die Benutzerrolle ist gelöscht.

Richtlinienprofile mit Rollen verbinden

Sie können Benutzerrollen mit Richtlinienprofilen verbinden. In diesem Fall basiert die Aktivierungsregel für dieses Richtlinienprofil auf der Rolle: das Richtlinienprofil wird für einen Benutzer aktiv, der über die festgelegte Rolle verfügt.

Beispielsweise verbietet die Richtlinie auf allen Geräten der Administrationsgruppe Programme zur GPS-Navigation. GPS-Navigation sind nur auf einem einzigen Gerät in der Administrationsgruppe "Benutzer" erforderlich, dem Gerät, dessen Inhaber als Kurier beschäftigt ist. In diesem Fall können Sie seinem Inhaber eine "Kurier"-Rolle zuweisen und dann einen Richtlinienprofil erstellen, das die Ausführung von GPS-Navigationssoftware nur auf den Geräten erlaubt, deren Inhabern die "Kurier"-Rolle zugewiesen ist. Alle anderen Richtlinieneinstellungen bleiben erhalten. Nur der Benutzer mit der Rolle "Kurier" hat die Erlaubnis, GPS-Navigationssoftware auszuführen. Wenn später einem weiteren Mitarbeiter die "Kurier"-Rolle zugewiesen wird, darf der neue Mitarbeiter ebenfalls Navigationssoftware auf den Geräten Ihrer Organisation ausführen. Das Ausführen von GPS-Navigationssoftware ist auf anderen Geräten in derselben Administrationsgruppe weiterhin verboten.

Um eine Rolle mit einem Richtlinienprofil zu verbinden, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Benutzer und Rollen** → **Rollen**.
2. Klicken Sie auf den Namen und die Rolle, die Sie mit einem Richtlinienprofil verbinden möchten.

   Das Fenster "Rolleneigenschaften" wird geöffnet, in dem die Registerkarte **Allgemein** ausgewählt ist.

3. Wählen Sie die Registerkarte **Einstellungen** aus und scrollen Sie nach unten zum Abschnitt **Richtlinien**.

4. Klicken Sie auf die Schaltfläche **Bearbeiten**.

5. Um die Rolle mit einem der folgenden Profile zu verbinden, gehen Sie wie folgt vor:

   - **Vorhandenes Richtlinienprofil**: Klicken Sie auf das Chevron-Symbol (>) neben dem entsprechenden Richtliniennamen und aktivieren Sie dann das Kontrollkästchen neben dem Profil, mit dem Sie die Rolle verbinden möchten.

   - **Neues Richtlinienprofil**:

     a. Aktivieren Sie das Kontrollkästchen neben der Richtlinie, für die Sie ein Profil erstellen möchten.

     b. Klicken Sie auf die Schaltfläche **Neues Richtlinienprofil**.

     c. Geben Sie den Namen des neuen Profils ein und passen Sie seine Einstellungen an.

     d. Klicken Sie auf die Schaltfläche **Speichern**.

     e. Aktivieren Sie das Kontrollkästchen neben dem neuen Profil.

6. Klicken Sie auf die Schaltfläche **Einer Rolle zuordnen**.

Das Profil wird mit der Rolle verbunden und in den Eigenschaften der Rolle angezeigt. Das Profil wird automatisch für alle Geräte übernommen, deren Inhabern die Rolle zugewiesen ist.

Ausdehnen von Benutzerrollen auf sekundäre Administrationsserver

Standardmäßig sind die Listen der Benutzerrollen des primären und der sekundären Administrationsserver voneinander unabhängig. Sie können die Anwendung so anpassen, dass die auf dem primären Administrationsserver erstellten Benutzerrollen automatisch auf alle sekundären Administrationsserver verteilt werden. Die Benutzerrollen können auch von einem sekundären Administrationsserver auf dessen eigene sekundäre Administrationsserver verteilt werden.

Um Benutzerrollen vom primären Administrationsserver auf die sekundären Administrationsserver zu verteilen:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wechseln Sie zum Abschnitt **Hierarchie der Administrationsserver**.

3. Aktivieren Sie die Option **Liste mit Rollen an sekundäre Administrationsserver weiterleiten** und klicken Sie anschließend auf die Schaltfläche **Speichern**.

Die Anwendung kopiert die Benutzerrollen des primären Administrationsservers auf die sekundären Administrationsserver.

Wenn die Option **Liste mit Rollen an sekundäre Administrationsserver weiterleiten** aktiviert ist und die Benutzerrollen verteilt werden, können sie auf den sekundären Administrationsservern nicht geändert oder gelöscht werden. Wenn Sie auf dem primären Administrationsserver eine neue Rolle erstellen oder eine bestehende ändern, werden die Änderungen automatisch auf die sekundären Administrationsserver kopiert. Wenn Sie auf dem primären Administrationsserver eine Benutzerrolle löschen, verbleibt diese Rolle danach auf den sekundären Administrationsservern, kann aber geändert oder gelöscht werden.

Die vom primären Administrationsserver an die sekundären Administrationsserver weitergeleiteten Rollen werden durch grüne Häkchen (✓) markiert. Diese Rollen können auf dem sekundären Administrationsserver nicht bearbeitet werden.

Wenn Sie eine Rolle auf dem primären Administrationsserver erstellen, während auf seinem sekundären Administrationsserver eine Rolle mit demselben Namen vorhanden ist, wird die neue Rolle auf den sekundären Administrationsserver kopiert und der Rollenname um einen Index erweitert, z. B. ~~1 oder ~~2 (der Index kann eine Zufallszahl sein).

Wenn Sie die Option **Liste mit Rollen an sekundäre Administrationsserver weiterleiten** deaktivieren, verbleiben alle Benutzerrollen auf den sekundären Administrationsservern, werden dabei jedoch von jeder Rolle auf dem primären Administrationsserver unabhängig. Nachdem sie unabhängig wurden, können die Benutzerrollen auf den sekundären Administrationsservern geändert oder gelöscht werden.

Kennwort des Benutzerkontos ändern

Sie können das Kennwort eines lokalen Benutzerkontos ändern. Dies kann nützlich sein, wenn ein Benutzer das Kennwort seines lokalen Kontos vergisst oder wenn eine geplante Kennwortänderung durchgeführt wird.

Die Kennwortänderung ist auch dann wirksam, wenn der Benutzer nicht beim Konto angemeldet ist. Sie können auch das Kennwort für das lokale Root-Konto ändern.

Diese Aufgabe kann nur auf Linux-Geräten ausgeführt werden.

So ändern Sie das Kennwort des lokalen Kontos für ausgewählte Geräte:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie im Feld **Aufgabentyp** den die Option **Kennwort des Benutzerkontos ändern (nur Linux)** aus.
4. Wählen Sie eine der folgenden Varianten aus:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

- **Geräteadressen manuell angeben oder aus Liste importieren**

  Sie können DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die Aufgabe zugewiesen werden soll.

  Diese Option können Sie beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

Die Aufgabe *Kennwort des Benutzerkontos ändern (nur Linux)* wird für die angegebenen Geräte erstellt. Wenn Sie Option **Aufgabe einer Administrationsgruppe zuweisen** ausgewählt haben, ist die Aufgabe eine Gruppenaufgabe.

5. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Auswahl an Geräten an.

   Die verfügbaren Einstellungen hängen von der im vorherigen Schritt ausgewählten Option ab.

6. Geben Sie im Schritt **Geben Sie den Namen des Benutzerkontos und das neue Kennwort an** die folgenden Einstellungen an:

   - Geben Sie im Feld **Name des Benutzerkontos** den Namen des Kontos an, für welches Sie das Kennwort ändern möchten.

   - Geben Sie im Feld **Neues Kennwort** das Kennwort an, das Sie für das im vorherigen Feld angegebene Benutzerkonto festlegen möchten.

     Wenn Sie die eingegebenen Zeichen sehen möchten, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie sie gedrückt.

   - Aktivieren Sie bei Bedarf das Kontrollkästchen **Dies ist ein Einmalkennwort (der Benutzer muss das Kennwort nach dem ersten Anmelden ändern)**.

     - **Dies ist ein Einmalkennwort (der Benutzer muss das Kennwort nach dem ersten Anmelden ändern)**

       Wenn dieses Kontrollkästchen aktiviert ist, wird der Benutzer nach der ersten Anmeldung aufgefordert, ein neues Kennwort festzulegen.

       Wenn dieses Kontrollkästchen deaktiviert ist, wird der Benutzer nach der ersten Anmeldung nicht aufgefordert, ein neues Kennwort festzulegen.

       Dieses Kontrollkästchen ist standardmäßig deaktiviert.

7. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um die Aufgabe zu erstellen und den Assistenten zu beenden.

   Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen, ändern oder bei Bedarf einen Startzeitplan für die Aufgabe konfigurieren.

8. Wählen Sie in der Aufgabenliste die von Ihnen erstellte Aufgabe aus und klicken Sie anschließend auf **Start**.

   Alternativ können Sie warten, bis die Aufgabe nach dem Zeitplan aus den Aufgabeneinstellungen gestartet wird.

Nach Abschluss der Aufgabe zur Kennwortänderung wird das Kennwort für das angegebene lokale Konto auf den ausgewählten Geräten geändert.

Um sicherzustellen, dass die Aufgaben zur Kennwortänderung korrekt ausgeführt werden, muss SELinux auf dem Benutzergerät deaktiviert sein.

Lokale Administratorrechte entziehen

Sie können den Benutzerkonten lokale Administratorrechte entziehen. Dadurch erhalten Sie mehr Kontrolle über die Benutzerkonten. Sie können beispielsweise die lokalen Administratorrechte entziehen, nachdem eine einmalige Zuweisung abgeschlossen wurde.

Beim Ausführen dieser Aufgabe wird überprüft, ob das angegebene lokale Benutzerkonto zu den Gruppen mit lokalen Administratoren gehört. Diese Gruppen werden in den Richtlinieneinstellungen des Administrationsagenten definiert. Sie können die Liste der Gruppen mit lokalen Administratoren in den Richtlinieneinstellungen des Administrationsagenten konfigurieren. Sie können die Liste der privilegierten Benutzerkonten auch mithilfe des **Bericht über privilegierte Gerätenutzer (nur Linux)** überprüfen.

Diese Aufgabe kann nur auf Linux-Geräten ausgeführt werden.

So entziehen Sie die lokalen Administratorrechte auf ausgewählten Geräten:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie im Feld **Aufgabentyp** die Option **Lokale Administratorrechte widerrufen (nur Linux)**.
4. Wählen Sie eine der folgenden Varianten aus:

   - **Aufgabe einer Administrationsgruppe zuweisen**

     Die Aufgabe wird den Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen angeben oder eine neue erstellen.

     Sie können diese Option beispielsweise für den Start einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die zu einer bestimmten Administrationsgruppe gehören.

     Wenn eine Aufgabe einer Administrationsgruppe zugewiesen ist, wird die Registerkarte **Sicherheit** im Fenster der Aufgabeneigenschaften nicht angezeigt, da Gruppenaufgaben den Sicherheitseinstellungen der entsprechenden Gruppen unterliegen.

   - **Geräteadressen manuell angeben oder aus Liste importieren**

     Sie können DNS-Namen, IP-Adressen und IP-Subnetze der Geräte angeben, denen die Aufgabe zugewiesen werden soll.

     Diese Option können Sie beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Beispielsweise können Sie eine bestimmte Anwendung auf den Geräten von Buchhaltern installieren oder Geräte in einem möglicherweise infizierten Subnetz untersuchen.

- **Aufgabe einer Geräteauswahl zuweisen**

  Die Aufgabe wird den Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen angeben.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

Die Aufgabe *Lokale Administratorrechte entziehen (nur Linux)* wird für die angegebenen Geräte erstellt. Wenn Sie die Option **Aufgabe einer Administrationsgruppe zuweisen** ausgewählt haben, ist die Aufgabe eine Gruppenaufgabe.

5. Geben Sie im Schritt **Gültigkeitsbereich der Aufgabe** eine Administrationsgruppe, Geräte mit bestimmten Adressen oder eine Auswahl an Geräten an.

   Die verfügbaren Einstellungen hängen von der im vorherigen Schritt ausgewählten Option ab.

6. Geben Sie in diesem Schritt des Assistenten die folgenden Einstellungen an:

   - Wählen Sie in der Einstellungsgruppe **Ausführungsmodus** den Ausführungsmodus aus:

     - **Lokale Administratorrechte von den aufgelisteten Benutzerkonten widerrufen**

       Wenn diese Option aktiviert ist, werden den angegebenen lokalen Benutzerkonten die lokalen Administratorrechte entzogen.

       Diese Option ist standardmäßig ausgewählt.

     - **Aufgelistete Benutzerkonten vom Widerruf der lokalen Administratorrechte ausschließen**

       Wenn diese Option ausgewählt ist, werden die lokalen Administratorrechte allen lokalen Benutzerkonten außer den angegeben entzogen.

       Diese Variante ist standardmäßig nicht ausgewählt.

   - Geben Sie die lokalen Benutzerkonten an:

     - Klicken Sie auf **Hinzufügen**.

     - Führen Sie im nächsten Fenster die folgenden Schritte aus:

       - Geben Sie im Feld **Benutzerkonto-Name** den Namen des lokalen Benutzerkontos an.

       - Wählen Sie in der Einstellungsgruppe **Aktion für das Benutzerkonto** (nur verfügbar, wenn die Option **Lokale Administratorrechte von den aufgelisteten Benutzerkonten widerrufen** ausgewählt ist) eine Aktion aus.

       - **Benutzerkonto beibehalten**

         Wenn diese Option ausgewählt ist, wird das lokale Benutzerkonto nicht gelöscht, nachdem die lokalen Administratorrechte entzogen wurden.

         Diese Option ist standardmäßig ausgewählt.

       - **Benutzerkonto löschen**

         Wenn diese Option ausgewählt ist, wird das lokale Benutzerkonto gelöscht, unabhängig davon, ob es über lokale Administratorrechte verfügt.

         Diese Variante ist standardmäßig nicht ausgewählt.

7. Klicken Sie im Schritt **Erstellung der Aufgabe abschließen** auf die Schaltfläche **Fertigstellen**, um die Aufgabe zu erstellen und den Assistenten zu beenden.

   Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit Aufgabeneinstellungen geöffnet. In diesem Fenster können Sie die Aufgabeneinstellungen überprüfen, ändern oder bei Bedarf einen Startzeitplan für die Aufgabe konfigurieren.

8. Wählen Sie in der Aufgabenliste die von Ihnen erstellte Aufgabe aus und klicken Sie anschließend auf **Start**.

   Alternativ können Sie warten, bis die Aufgabe nach dem Zeitplan aus den Aufgabeneinstellungen gestartet wird.

Nachdem die Aufgabe zum Entziehen lokaler Administratorrechte abgeschlossen ist, wurden den angegebenen lokalen Benutzerkonten auf den festgelegten Geräten die lokalen Administratorrechte entzogen.

Kerberos-Domänenauthentifizierung konfigurieren

Mit Kaspersky Security Center Linux können Sie die Domänenauthentifizierung über das Kerberos-Protokoll verwenden. Die Domänenauthentifizierung erlaubt Ihnen, die sichere Authentifizierung in Kaspersky Security Center Web Console zu aktivieren, ohne das Kennwort im Unternehmensnetzwerk erneut eingeben zu müssen (Single Sign-on).

Sie müssen zunächst Ihren Domänencontroller konfigurieren, um Kerberos zu verwenden und eine keytab-Datei zu erzeugen. Weitere Informationen darüber finden Sie in der Dokumentation Ihres Domänencontrollers.

SCRIL (für interaktive Anmeldung ist eine Smartcard erforderlich) wird für Microsoft Active Directory unterstützt.

Generieren einer keytab-Datei für FreeIPA und AldPro

So generieren Sie eine keytab-Datei :

1. Erstellen Sie ein Benutzerkonto, das von IAM für den Zugriff auf den Domänencontroller verwendet werden soll.

2. Wenn sich der Administrationsserver außerhalb der FreeIPA-/AldPro-Domäne befindet, fügen Sie den DNS-Eintrag und den Host-Eintrag hinzu:

   ```
   ipa dnsrecord-add <zoneName> <recordName> --a-rec < IP-Adresse des Administrationsservers >
   ```

   ```
   ipa host-add --password=<password> < Adresse des Hosts des Administrationsservers >
   ```

3. Geben Sie den PAC-Typ an, wenn Sie den HTTP-Dienst für den Administrationsserver erstellen:

   ```
   ipa service-add HTTP/< FQDN des Hosts des Administrationsservers >@< DOMÄNE IN GROSSBUCHSTABEN > --ok-to-auth-as-delegate=true --pac-type PAD
   ```

4. Geben Sie das Benutzerkonto für die Authentifizierung an:

   ```
   ipa service-allow-retrieve-keytab HTTP/< Adresse des Hosts des Administrationsservers >@< DOMÄNE IN GROSSBUCHSTABEN > --user=<user>
   ```

5. Exportieren Sie die keytab-Datei.

   ```
   ipa-getkeytab -s < Adresse des Domänencontrollers > -p HTTP/< Adresse des Hosts des Administrationsservers >@< DOMÄNE IN GROSSBUCHSTABEN > -k /tmp/h.keytab
   ```

Generieren einer keytab-Datei für Microsoft Active Directory

So generieren Sie eine keytab-Datei :

1. Erstellen Sie ein Benutzerkonto, das von IAM für die Kommunikation mit dem Domänencontroller verwendet werden soll.
2. Aktivieren Sie für das Benutzerkonto die folgenden Optionen:
   - **Der Benutzer darf das Kennwort nicht ändern**
   - **Kerberos AES 256-Bit-Verschlüsselung**

   Sie können die Option **Kennwort läuft nie ab** aktivieren, um das erneute Ausstellen der keytab-Datei nach jedem Ablauf des Kennworts zu vermeiden.
3. Fügen Sie dem Benutzerkonto ein Service Principal Name (SPN) hinzu:

   ```
   setspn -S HTTP/< FQDN des Hosts des Administrationsservers > < DOMÄNE IN GROSSBUCHSTABEN >\<user>
   ```
4. Exportieren Sie die keytab-Datei.

   ```
   ktpass -out C:\<folder>\< Name der keytab-Datei > -princ HTTP/< FQDN des Hosts des Administrationsservers >@< DOMÄNE IN GROSSBUCHSTABEN > -mapuser < DOMÄNE IN GROSSBUCHSTABEN >\<user> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass <password> -mapop set
   ```

Generieren einer keytab-Datei für Samba

So generieren Sie eine keytab-Datei :

1. Erstellen Sie ein Benutzerkonto, das von IAM für die Kommunikation mit dem Domänencontroller verwendet werden soll:

   ```
   samba-tool user add <user>
   ```
2. Fügen Sie dem Benutzerkonto den SPN hinzu:

   ```
   samba-tool spn add HTTP/< FQDN des Hosts des Administrationsservers > <user>
   ```
3. Exportieren Sie die keytab-Datei.

   ```
   samba-tool domain exportkeytab /tmp/file.keytab --principal=HTTP/< FQDN des Hosts des Administrationsservers >
   ```

Aktivieren Sie die Kerberos-Domänenauthentifizierung

So aktivieren Sie die Kerberos-Domänenauthentifizierung:

1. Führen Sie eine Abfrage des Domänencontrollers durch.
2. Wechseln Sie im Hauptmenü zu **Einstellungen** → **Single Sign-On**.
3. Aktivieren Sie die Option **Kerberos-Authentifizierung**.

4. Laden Sie die keytab-Datei hoch.

5. Weisen Sie Domänenbenutzern eine Rolle zu, die ihnen Zugriff auf die Kaspersky Security Center Web Console ermöglicht.

   Die Kerberos-Domänenauthentifizierung ist für Domänenbenutzer aktiviert.

Datenbanken und Programme von Kaspersky aktualisieren

Dieser Abschnitt beschreibt die Schritte, die Sie für ein regelmäßiges Update durchführen müssen:

- Kaspersky-Datenbanken und Programm-Module
- Installierte Kaspersky-Anwendungen, einschließlich der Komponenten von Kaspersky Security Center Linux und der Sicherheitsanwendungen

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Szenario: Datenbanken und Programme von Kaspersky regelmäßig aktualisieren

Dieser Abschnitt enthält ein Szenario zum regelmäßigen Update der Datenbanken, Softwaremodule und Anwendungen von Kaspersky. Nachdem Sie das Szenario "Netzwerkschutz konfigurieren" abgeschlossen haben, müssen Sie die Verlässlichkeit des Schutzsystems aufrecht erhalten, um sicherzustellen, dass die Administrationsserver und die verwalteten Geräte dauerhaft gegen verschiedene Bedrohungen wie Viren, Netzwerkangriffe und Phishing-Attacken geschützt sind.

Der Netzwerkschutz bleibt auf dem neuesten Stand, wenn folgende Komponenten regelmäßig aktualisiert werden:

- Kaspersky-Datenbanken und Programm-Module
- Installierte Kaspersky-Anwendungen, einschließlich der Komponenten von Kaspersky Security Center Linux und der Sicherheitsanwendungen

Wenn Sie dieses Szenario abschließen, können Sie sicher sein, dass:

- Ihr Netzwerk durch die aktuellsten Kaspersky-Anwendungen, einschließlich der Komponenten von Kaspersky Security Center Linux und der Sicherheitsanwendungen, geschützt ist.
- die Antiviren-Datenbanken und andere, für die Sicherheit des Netzwerks kritische Kaspersky-Datenbanken, immer auf dem neuesten Stand sind.

Erforderliche Vorrausetzungen

Die verwalteten Geräte benötigen eine Verbindung zum Administrationsserver. Wenn keine Verbindung besteht, können Sie das Update der Kaspersky-Datenbanken und der Programm-Module auch manuell oder direkt über die Kaspersky-Update-Server durchführen.

Der Administrationsserver muss eine Verbindung zum Internet haben.

Bevor Sie beginnen, stellen Sie sicher, dass Sie:

1. die Sicherheitsanwendungen von Kaspersky gemäß dem Szenario zur Verteilung von Kaspersky-Anwendungen via Kaspersky Security Center Web Console auf den verwalteten Geräten verteilt haben.
2. alle notwendigen Richtlinien, Richtlinienprofile und Aufgaben entsprechend dem Szenario "Konfiguration des Netzwerkschutzes" konfiguriert haben.
3. in Übereinstimmung mit der Anzahl der verwalteten Geräte und der Netzwerktopologie eine geeignete Anzahl an Verteilungspunkten zugewiesen haben.

Das Update der Datenbanken und Anwendungen von Kaspersky erfolgt in mehreren Schritten:

1. **Auswählen eines Update-Schemas**

   Es existieren verschiedene Schemata, mit denen Sie Updates für Sicherheitsanwendungen installieren können. Wählen Sie ein Schema oder mehrere Schemas, welche die Anforderungen Ihres Netzwerks am besten erfüllen.

2. **Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen**

   Diese Aufgabe wird automatisch vom Schnellstartassistenten des Kaspersky Security Centers erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe jetzt.

   Diese Aufgabe wird benötigt, um Updates von den Kaspersky-Update-Servern in die Datenverwaltung des Administrationsservers zu laden, und um die Updates der Kaspersky-Datenbanken und Programm-Module des Kaspersky Security Centers Linux auszuführen. Nachdem die Updates heruntergeladen wurden, können Sie an die verwalteten Geräte weitergegeben werden.

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt, werden die Updates aus der Datenverwaltung des Administrationsservers in die Datenverwaltungen der Verteilungspunkte geladen. In diesem Fall laden die verwalteten Geräte, die sich im Bereich eines Verteilungspunktes befinden, die Updates aus der Datenverwaltung des Verteilungspunktes, anstatt aus der Datenverwaltung des Administrationsservers.

   Anleitungen: Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen

3. **Aufgabe zum Download von Updates in die Datenverwaltung auf Verteilungspunkte erstellen (optional)**

   Standardmäßig werden die Updates von den Verteilungspunkten vom Administrationsserver heruntergeladen. Sie können Kaspersky Security Center Linux so konfigurieren, dass die Verteilungspunkte die Updates direkt von den Kaspersky-Update-Servern herunterladen. Der direkte Download in die Datenverwaltung der Verteilungspunkte ist dann vorzuziehen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt und die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* erstellt wurde, laden die Verteilungspunkte Updates von den Kaspersky-Update-Servern herunter, und nicht von der Datenverwaltung des Administrationsservers.

   Anleitung: Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen

4. **Konfigurieren der Verteilungspunkte**

   Wenn Ihr Netzwerk über zugewiesene Verteilungspunkte verfügt, stellen Sie sicher, dass die Option **Aktiviert** in den Einstellungen aller benötigten Verteilungspunkte aktiviert ist. Wenn diese Option für einen Verteilungspunkt deaktiviert ist, laden die Geräte, die sich im Bereich dieses Verteilungspunktes befinden, die Updates von der Datenverwaltung des Administrationsservers herunter.

5. **Optimieren des Update-Vorgangs durch Diff-Dateien (optional)**

   Sie können den Datenverkehr zwischen dem Administrationsserver und den verwalteten Geräten optimieren, indem Sie Diff-Dateien verwenden. Wenn diese Funktion aktiviert ist, laden der Administrationsserver oder ein Verteilungspunkt im Gegensatz zu ganzen Kaspersky-Datenbank-Dateien oder Programm-Modulen nur Diff-Dateien herunter. Eine Diff-Datei beschreibt den Unterschied zwischen zwei Versionen der Datei einer Datenbank oder eines Programm-Moduls. Deswegen benötigt eine Diff-Datei weniger Platz als eine ganze Datei. Dies resultiert in einem verringerten Datenverkehr zwischen dem Administrationsserver oder Verteilungspunkt und den verwalteten Geräten. Um diese Funktion zu nutzen, aktivieren Sie die Option **Diff-Dateien herunterladen** in den Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und/oder der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*.

   Anleitung: Diff-Dateien zum Update von Kaspersky-Datenbanken und Programm-Modulen verwenden

6. **Konfiguration der automatischen Installation von Updates für die Sicherheitsanwendungen**

   Erstellen Sie die *Update*-Aufgaben für verwaltete Anwendungen, um zeitnahe Updates für die Software-Module und Kaspersky-Datenbanken (einschließlich der Antiviren-Datenbanken) zu gewährleisten. Damit Updates immer rechtzeitig erfolgen, sollten Sie beim Konfigurieren des Aufgabenplans die Option **Nach dem Download von Updates in die Datenverwaltung** aktivieren.

   Wenn ein Update eine Überprüfung und ein Akzeptieren des Endbenutzer-Lizenzvertrags benötigt, müssen Sie die Bestimmungen zuerst akzeptieren. Danach kann das Update an die verwalteten Geräte verteilt werden.

7. **Updates für verwaltete Kaspersky-Anwendungen genehmigen und ablehnen**

   Standardmäßig besitzen heruntergeladene Programm-Updates den Status *Nicht definiert*. Sie können den Status auf *Genehmigt* oder *Abgelehnt* ändern. Genehmigte Updates werden immer installiert. Wenn ein Update für eine verwaltete Kaspersky-Anwendung das Überprüfen und Akzeptieren des Endbenutzer-Lizenzvertrags erfordert, müssen Sie die Bestimmungen zuvor akzeptieren. Danach kann das Update an die verwalteten Geräte verteilt werden. Updates, für die Sie den Status *Abgelehnt* gewählt haben, werden auf den Geräten nicht installiert. Wenn ein abgelehntes Update für eine verwaltete Anwendung bereits vor der Ablehnung installiert wurde, wird Kaspersky Security Center Linux versuchen, dieses Update von allen Geräten zu deinstallieren.

   Das Genehmigen und Ablehnen von Updates ist nur für Administrationsagenten und verwaltete Kaspersky-Anwendungen verfügbar, die auf Windows- oder Linux-basierten Client-Geräten installiert sind. Eine nahtlose Aktualisierung wird von den folgenden Komponenten nicht unterstützt: Administrationsserver, Kaspersky Security Center Web Console und Web-Plug-ins zur Verwaltung.

   Anleitung: Genehmigen und Ablehnen von Programm-Updates

   Nach einem Update des Administrationsagenten werden Sie möglicherweise aufgefordert, die verwalteten Geräte neu zu starten. Wenn der Hinweis über einen erforderlichen Neustart angezeigt wird, klicken Sie in dem Hinweis auf den Link **Geräte anzeigen**, aktivieren Sie die Kontrollkästchen neben den neu zu startenden Geräten und klicken Sie anschließend auf die Schaltfläche **Neu starten**, um das Update des Administrationsagenten abzuschließen.

Ergebnisse

Nach Abschluss des Szenarios ist Kaspersky Security Center Linux so konfiguriert, dass die Kaspersky-Datenbanken aktualisiert werden, nachdem die Updates in die Datenverwaltung des Administrationsservers heruntergeladen wurden. Anschließend können Sie mit der Überwachung des Netzwerkstatus fortfahren.

Über das Aktualisieren der Datenbanken, Software-Module und Programme von Kaspersky

Um sicherzustellen, dass der Schutz Ihrer Administrationsserver und verwalteten Geräte auf dem neuesten Stand ist, müssen Sie zeitnah Updates bereitstellen für:

- Kaspersky-Datenbanken und Programm-Module

  Vor dem Herunterladen von Kaspersky-Datenbanken und Softwaremodulen überprüft Kaspersky Security Center Linux, ob die Kaspersky-Server erreichbar sind. Wenn der Zugriff auf die Server über systemspezifisches DNS nicht möglich ist, verwendet das Programm öffentliche DNS-Server. Dies ist erforderlich, um sicherzustellen, dass die Antiviren-Datenbanken aktualisiert werden und das Sicherheitsniveau für die verwalteten Geräte beibehalten wird.

- Installierte Kaspersky-Anwendung, einschließlich der Komponenten von Kaspersky Security Center Linux und der Sicherheitsanwendungen

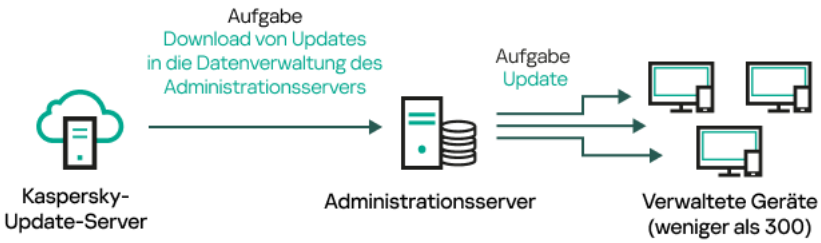
  Kaspersky Security Center Linux ermöglicht Ihnen die automatische Aktualisierung des Administrationsagenten und der Kaspersky-Anwendungen auf Geräten mit Windows und Linux. Ein nahtloses Update der folgenden Komponenten wird nicht unterstützt: Administrationsserver, Kaspersky Security Center Web Console und Web-Plug-ins zur Verwaltung. Um diese Komponenten zu aktualisieren, müssen Sie die jeweils aktuellste Version von der Kaspersky-Website herunterladen und anschließend manuell installieren.

Abhängig von der Konfiguration Ihres Netzwerks können Sie die folgenden Schemata für das Herunterladen und Verteilen der erforderlichen Updates auf die verwalteten Geräte verwenden:

- Durch Verwendung einer einzelnen Aufgabe: *Download von Updates in die Datenverwaltung des Administrationsservers*
- Durch Verwendung zweier Aufgaben:
  - Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*
  - Die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*
- Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server
- Direkt von den Kaspersky-Update-Servern an Kaspersky Endpoint Security auf den verwalteten Geräten
- Über einen lokalen Ordner oder Netzwerkordner, wenn der Administrationsserver keine Internetverbindung hat

Verwenden der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers

In diesem Schema lädt Kaspersky Security Center Linux über die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* Updates herunter. In kleinen Netzwerken, die weniger als 300 verwaltete Geräte in einem einzelnen Netzwerksegment oder weniger als 10 verwaltete Geräte in jedem Netzwerksegment enthalten, werden die Updates direkt aus der Datenverwaltung des Administrationsservers auf die verwalteten Geräte verteilt (siehe Abbildung unten).



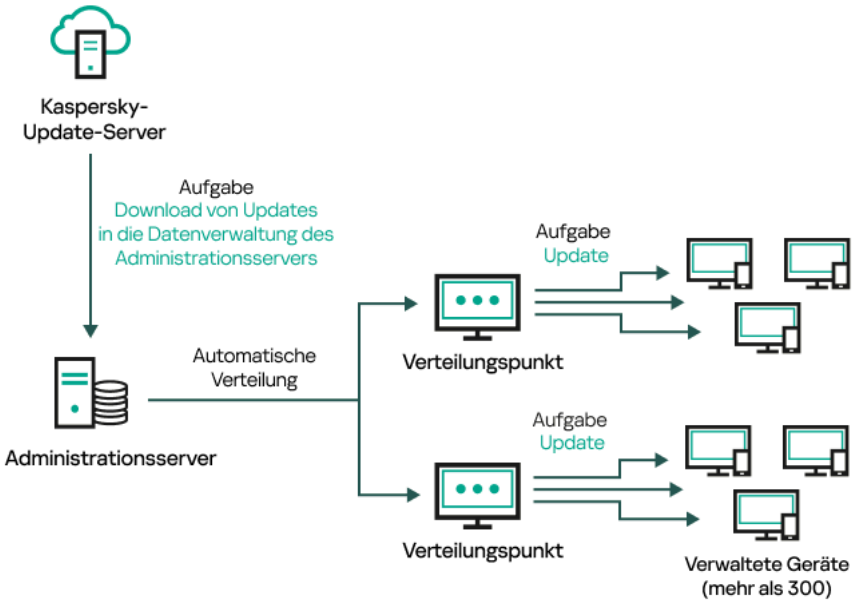
Update mithilfe der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ohne Verteilungspunkte

Sie können nicht nur die Kaspersky-Update-Server als Update-Quelle verwenden, sondern auch einen lokalen Ordner oder einen Netzwerkordner.

Standardmäßig verwendet der Administrationsserver zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können Administrationsserver so einrichten, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

Wenn Ihr Netzwerk 300 oder mehr verwaltete Geräte in einem einzigen Netzwerksegment enthält oder wenn Ihr Netzwerk aus mehreren Netzwerksegmenten mit mehr als 9 verwalteten Geräten in jedem Netzwerksegment besteht, empfehlen wir Ihnen, Verteilungspunkte zu verwenden, um die Updates auf die verwalteten Geräte zu übertragen (siehe Abbildung unten). Verteilungspunkte reduzieren die Belastung des Administrationsservers und optimieren den Datenverkehr zwischen dem Administrationsserver und den verwalteten Geräten. Sie können die Anzahl und Konfiguration der für Ihr Netzwerk benötigten Verteilungspunkte berechnen.

In diesem Schema werden die Updates automatisch aus der Datenverwaltung des Administrationsservers in die Datenverwaltungen der Verteilungspunkte heruntergeladen. Die verwalteten Geräte, die zum Umfang eines Verteilungspunkts gehören, laden die Updates aus der Datenverwaltung des Verteilungspunkts anstelle der Datenverwaltung des Administrationsservers herunter.



Update mithilfe der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* mit Verteilungspunkten

Nach Abschluss der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* werden die Updates für die Kaspersky-Datenbanken und die Programm-Module für Kaspersky Endpoint Security in die Datenverwaltung des Administrationsservers heruntergeladen. Diese Updates werden durch die *Update-Aufgabe* von Kaspersky Endpoint Security für Windows installiert.

Die Aufgabe zum *Download von Updates in die Datenverwaltung des Administrationsservers* steht auf virtuellen Administrationsservern nicht zur Verfügung. In der Datenverwaltung des virtuellen Administrationsservers werden Updates angezeigt, die auf den primären Administrationsserver heruntergeladen wurden.

Sie können die Updates, die auf Funktionsfähigkeit und Fehler geprüft werden sollen, auf einer Reihe von Testgeräten konfigurieren. Wenn die Überprüfung erfolgreich ist, werden die Updates an andere verwaltete Geräte verteilt.

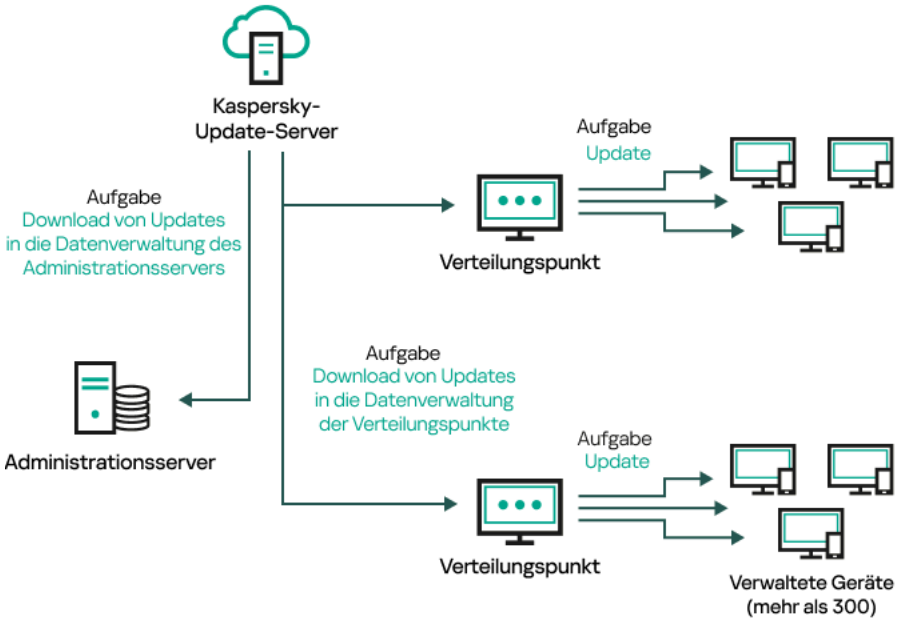
Jede Anwendung von Kaspersky fordert die erforderlichen Updates vom Administrationsserver an. Der Administrationsserver aggregiert diese Anforderungen und lädt nur die Aktualisierungen herunter, die von einer Anwendung angefordert werden. Dadurch wird sichergestellt, dass die gleichen Updates nicht mehrmals heruntergeladen werden und unnötige Updates überhaupt nicht heruntergeladen werden. Bei der Ausführung der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* der Administrationsserver die folgenden Informationen automatisch an Kaspersky-Update-Server, um das Herunterladen von relevanten Versionen der Kaspersky-Datenbanken und Programm-Module sicherzustellen:

- Anwendungs-ID und Version der Anwendung
- Setup-ID der Anwendung
- ID des aktiven Schlüssels
- Ausführungs-ID der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*

Keine der übermittelten Informationen enthält persönliche oder andere vertrauliche Daten. AO Kaspersky Lab schützt die erhaltenen Informationen in Übereinstimmung mit den geltenden gesetzlich festgelegten Anforderungen.

Verwendung von zwei Aufgaben: Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers und Aufgabe Updates in die Datenverwaltung der Verteilungspunkte herunterladen

Sie können Updates für die Datenverwaltungen der Verteilungspunkte direkt von den Update-Servern von Kaspersky anstelle der Datenverwaltung des Administrationsservers herunterladen und die Updates dann auf die verwalteten Geräte verteilen (siehe Abbildung unten). Der direkte Download in die Datenverwaltung der Verteilungspunkte ist dann vorzuziehen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.



Update mithilfe der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen*

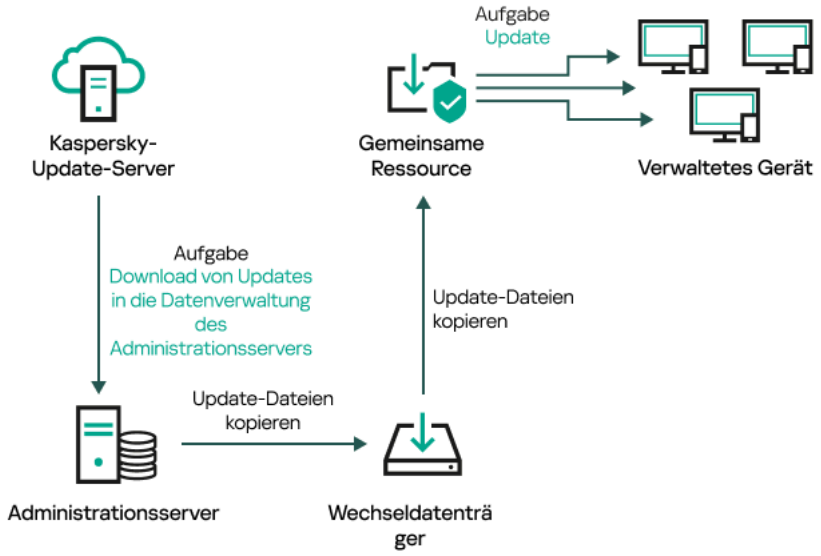
Standardmäßig verwenden der Administrationsserver und die Verteilungspunkte zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können den Administrationsserver und/oder die Verteilungspunkte so konfigurieren, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls verwendet wird.

Um dieses Schema zu implementieren, erstellen Sie die Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* zusätzlich zur Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*. Danach laden die Verteilungspunkte die Updates von den Kaspersky Update-Servern herunter und nicht von der Datenverwaltung des Administrationsservers.

Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* wird auch für dieses Schema benötigt, da mit dieser Aufgabe Datenbanken und Softwaremodule von Kaspersky für das Kaspersky Security Center Linux heruntergeladen werden können.

Manuell über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

Wenn die Client-Geräte keine Verbindung zum Administrationsserver haben, können Sie einen lokalen Ordner oder eine freigegebene Ressource als Quelle für das Update von Kaspersky-Datenbanken, -Softwaremodulen und -Anwendungen verwenden. In diesem Schema müssen Sie die erforderlichen Updates aus der Datenverwaltung des Administrationsservers auf einen Wechseldatenträger und dann in den lokalen Ordner oder die als Update-Quelle in den Einstellungen von Kaspersky Endpoint Security angegebene freigegebene Ressource kopieren (siehe Abbildung unten).



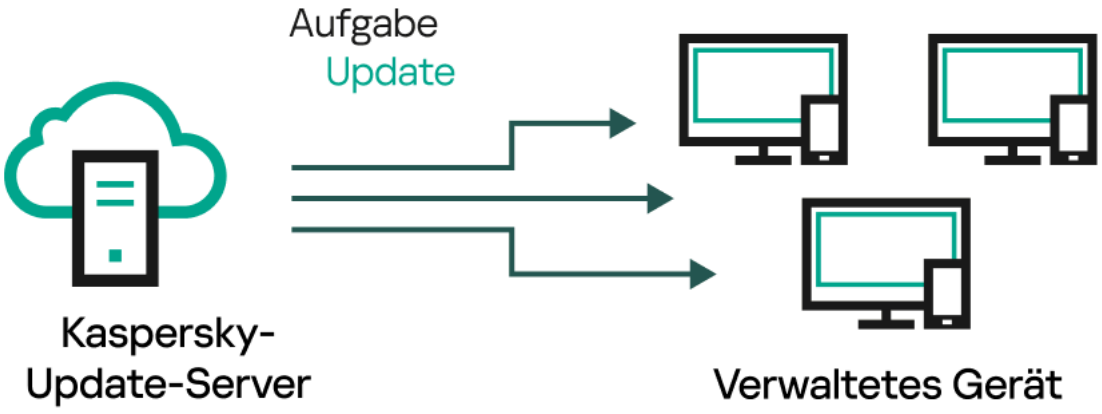
Manuelles Upgrade über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

Weitere Informationen zu Update-Quellen in Kaspersky Endpoint Security finden Sie in den folgenden Hilfen:

- Hilfe zu Kaspersky Endpoint Security für Linux
- Hilfe zu Kaspersky Endpoint Security für Windows

Direkt von den Kaspersky-Update-Servern an Kaspersky Endpoint Security auf den verwalteten Geräten

Auf den verwalteten Geräten können Sie Kaspersky Endpoint Security so konfigurieren, dass Updates direkt von den Updateservern von Kaspersky empfangen werden (siehe Abbildung unten).



Updates von Sicherheitsanwendungen direkt von Kaspersky Update-Servern aus

In diesem Schema verwendet die Sicherheitsanwendung nicht die von Kaspersky Security Center Linux bereitgestellte Datenverwaltung. Um Updates direkt von den Kaspersky-Update-Servern zu erhalten, geben Sie in der Sicherheitsanwendung die Kaspersky-Update-Server als Update-Quelle an. Weitere Informationen zu diesen Einstellungen finden Sie in den folgenden Hilfen:

- Hilfe zu Kaspersky Endpoint Security für Linux
- Hilfe zu Kaspersky Endpoint Security für Windows

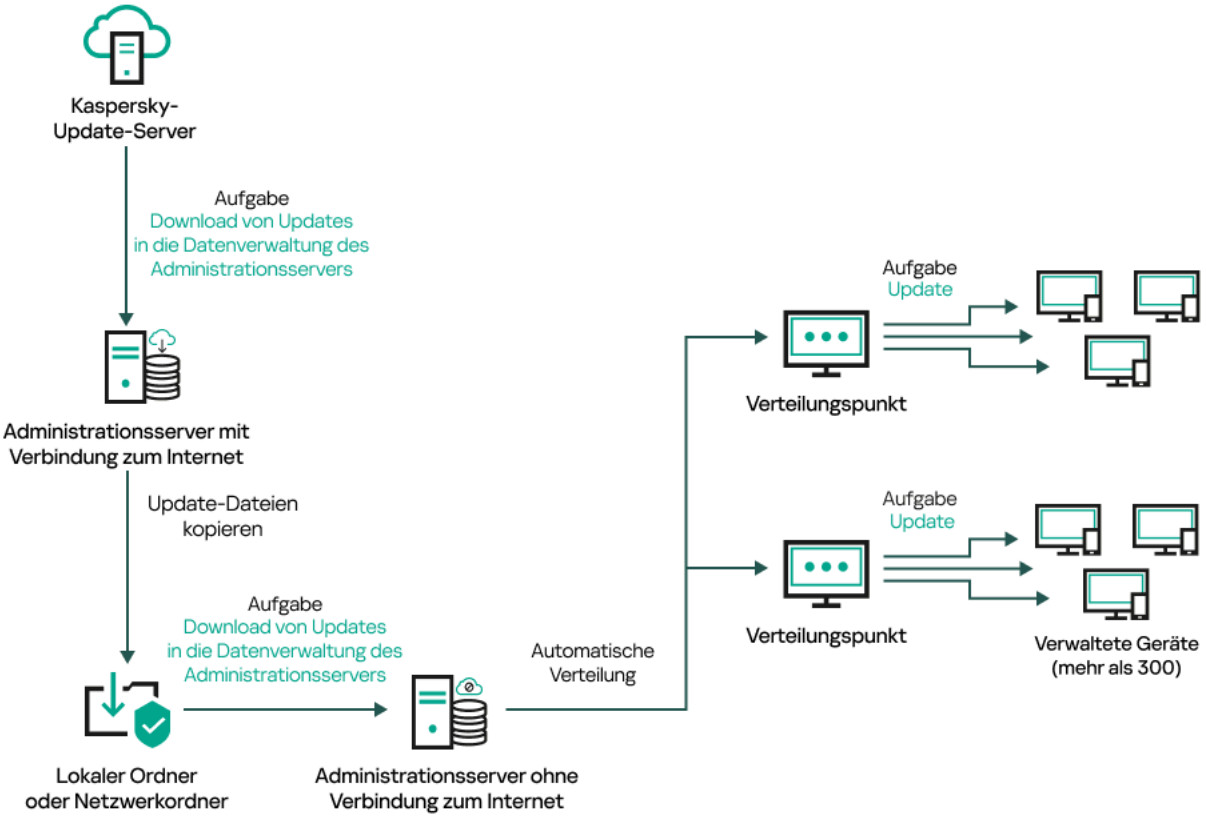
Über einen lokalen Ordner oder Netzwerkordner, wenn der Administrationsserver keine Internetverbindung hat

Wenn der Administrationsserver keine Internetverbindung hat, können Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* zum Herunterladen von Updates aus einem lokalen oder Netzwerkordner konfigurieren. In diesem Fall müssen Sie die erforderlichen Update-Dateien von Zeit zu Zeit in den angegebenen Ordner kopieren. Beispielsweise können Sie die erforderlichen Update-Dateien aus einer der folgenden Quellen kopieren:

- Administrationsserver mit Internetverbindung (siehe Abbildung unten)

  Da ein Administrationsserver nur die Updates herunterlädt, die von den Sicherheitsanwendungen angefordert werden, müssen die Gruppen der Sicherheitsanwendungen, die von den Administrationsservern verwaltetet werden – d. h. von dem mit Internetverbindung und dem ohne Internetverbindung – übereinstimmen.

  Wenn der von Ihnen zum Herunterladen von Updates verwendete Administrationsserver die Version 13.2 besitzt, öffnen Sie die Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und aktivieren Sie anschließend die Option **Updates nach altem Schema herunterladen**.



Aktualisieren mittels eines lokalen Ordners oder Netzwerkordners, wenn der Administrationsserver keine Internetverbindung hat

- Kaspersky Update Utility

  Da dieses Tool das alte Schema zum Herunterladen von Updates verwendet, öffnen Sie die Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und aktivieren Sie anschließend die Option *Updates nach altem Schema herunterladen*. Bei Bedarf können Sie die Option *Update-Anforderungsdatei automatisch herunterladen* auch so konfigurieren, dass vom Kaspersky Update Utility nur die erforderlichen Updates heruntergeladen werden.

Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen

Die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ist erforderlich, um die Updates für Datenbanken und Anwendungsmodule von Kaspersky-Sicherheitsanwendungen von den Kaspersky-Update-Servern in die Administrationsserver-Datenverwaltung herunterzuladen.

Der Schnellstartassistent von Kaspersky Security Center erstellt automatisch die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* für den Administrationsserver. In der Aufgabenliste kann nur eine Aufgabe des Typs *Download von Updates in die Datenverwaltung des Administrationsservers* vorhanden sein. Sie können diese Aufgabe erneut erstellen, wenn sie aus der Aufgabenliste des Administrationsservers entfernt wurde.

Nachdem die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* abgeschlossen und die Updates heruntergeladen wurden, können diese an die verwalteten Geräte weitergegeben werden.

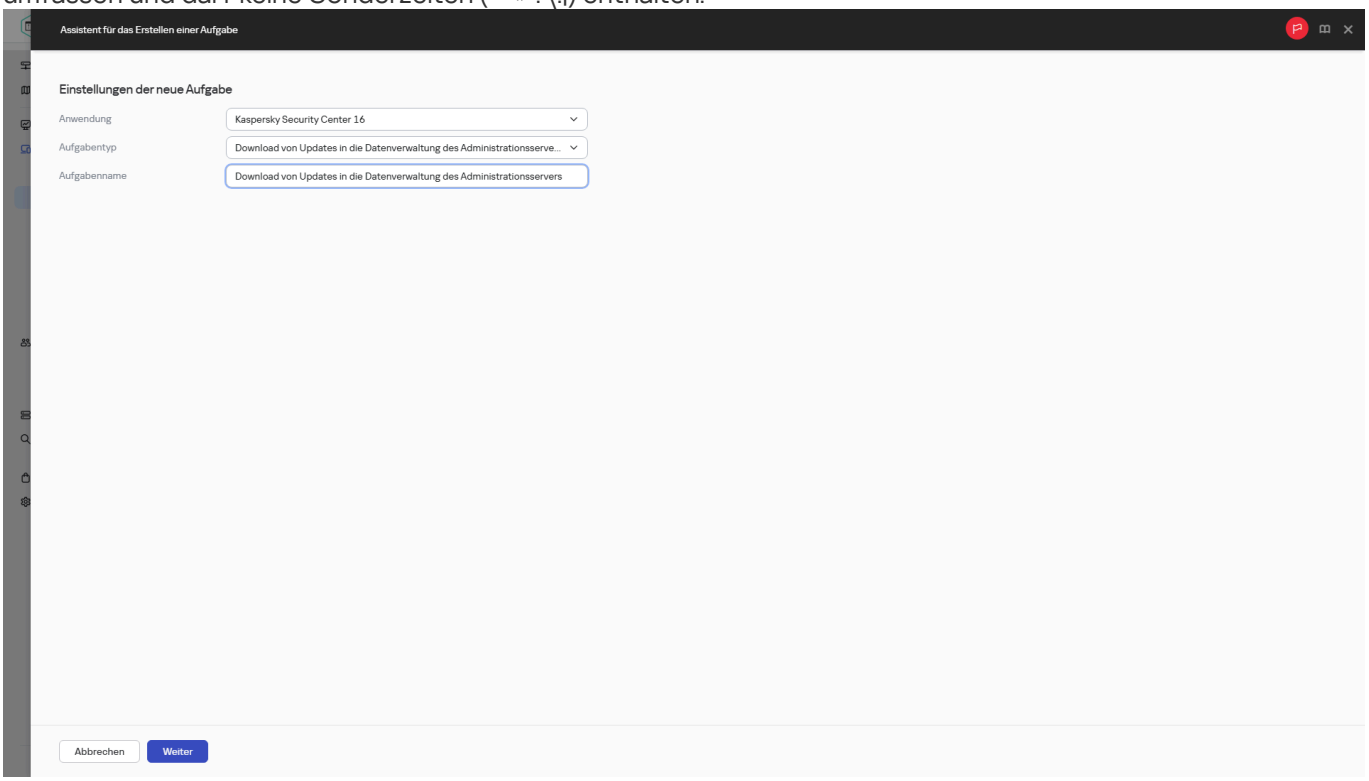
Bevor Sie Updates an die verwalteten Geräte weiterleiten, können Sie die Aufgabe zur *Update-Prüfung* ausführen. Dadurch können Sie sicherstellen, dass der Administrationsserver die heruntergeladenen Updates ordnungsgemäß installiert und die Sicherheitsstufe durch etwaige Updates nicht verringert wird. Um sie vor dem Verteilen zu überprüfen, konfigurieren Sie die Option **Update-Prüfung ausführen** in den Einstellungen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*.

Um die Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers zu erstellen:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Download von Updates in die Datenverwaltung des Administrationsservers**.

4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.



Erstellen der Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers

5. Auf der Seite **Erstellung der Aufgabe abschließen** können Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktivieren, um das Fenster mit den Aufgabeneigenschaften zu öffnen und die Aufgabeneinstellungen zu ändern. Alternativ können Sie Aufgabeneinstellungen jederzeit später konfigurieren.



Abschluss der Aufgabenerstellung

6. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.

7. Um das Fenster mit den Aufgabeneigenschaften zu öffnen, klicken Sie auf den Namen der erstellten Aufgabe.

8. Geben Sie im Fenster mit den Aufgabeneigenschaften auf der Registerkarte **Anwendungseinstellungen** die folgenden Einstellungen an:

- **Update-Quellen**

  Folgende Update-Quellen können verwenden:

  - Kaspersky-Update-Server
  - Primärer Administrationsserver
  - Lokaler Ordner oder Netzwerkordner

    Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben. Der Pfad des Ordners hängt vom Betriebssystem auf dem Gerät ab. Da sich der lokale Ordner auf einem Linux-basierten Administrationsserver befindet, müssen Sie den POSIX-Pfad angeben. Beispiel: /Pfad/zum/Verzeichnis.

    Wenn Sie einen Netzwerkordner auswählen, der sich auf einem Linux-Administrationsserver befindet, müssen Sie vorher durch das Mounten des Ordners sicherstellen, dass von dem Gerät mit installiertem Administrationsserver auf den Netzwerkordner zugegriffen werden kann. Der Zugriff auf den Ordner erfolgt über das SMB-Protokoll.

  In der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und der Aufgabe *Download von Updates in die Datenverwaltung der Verteilungspunkte* funktioniert die Benutzerauthentifizierung nicht, wenn Sie einen kennwortgeschützten lokalen Ordner oder Netzwerkordner als Update-Quelle auswählen. Um dieses Problem zu beheben, stellen Sie zuerst den kennwortgeschützten Ordner bereit und geben Sie dann die erforderlichen Anmeldedaten an, z. B. über das Betriebssystem. Danach können Sie diesen Ordner als Update-Quelle in einer Aufgabe für Update-Downloads auswählen. Für Kaspersky Security Center Linux müssen Sie keine Anmeldedaten eingeben.

- **Ordner zum Speichern von Updates**

  Der Pfad zum angegebenen Ordner, in dem die bezogenen Updates gespeichert werden. Sie können den Pfad des angegebenen Ordners in die Zwischenablage kopieren. Für eine Gruppenaufgabe können Sie den Pfad eines angegebenen Ordners nicht ändern.

- **Update der sekundären Administrationsserver erzwingen**

  Wenn diese Option aktiviert ist, startet der Administrationsserver die Update-Aufgaben auf den sekundären Administrationsservern sobald neue Updates heruntergeladen werden. Update-Aufgaben werden unter Verwendung der Update-Quellen gestartet, die in den Aufgabeneigenschaften auf den sekundären Administrationsservern konfiguriert ist.

  Wenn diese Option deaktiviert ist, werden die Update-Aufgaben auf den sekundären Administrationsservern gemäß ihren Zeitplänen gestartet.

  Diese Option ist standardmäßig deaktiviert.

- **Heruntergeladene Updates in zusätzliche Ordner kopieren**

  Nachdem der Administrationsserver Updates empfängt, kopiert er sie in die angegebenen Ordner. Verwenden Sie diese Option, wenn Sie die Verteilung von Updates in Ihrem Netzwerk manuell verwalten möchten.

Sie können diese Option beispielsweise in der folgenden Situation verwenden: Das Netzwerk Ihres Unternehmens besteht aus mehreren unabhängigen Subnetzen, wobei Geräte in den einzelnen Subnetzen über keinen Zugriff auf andere Subnetze verfügen. Allerdings haben Geräte in allen Teilnetzen Zugriff auf eine gemeinsame Netzwerkfreigabe. In diesem Fall müssen Sie den Administrationsserver in einem der Subnetze einrichten, um Updates von den Kaspersky-Update-Servern herunterzuladen. Aktivieren Sie diese Option und geben Sie dann diese Netzwerkfreigabe an. Geben Sie bei heruntergeladenen Updates der Repository-Aufgaben für andere Administrationsserver die gleiche Netzwerkfreigabe wie für die Update-Quelle an.

Wenn Sie auswählen, dass die Updates in einen lokalen Ordner kopiert werden sollen, müssen Sie einen Ordner auf dem Gerät mit dem installierten Administrationsserver angeben. Der Pfad des Ordners hängt vom Betriebssystem auf dem Gerät ab. Da sich der lokale Ordner auf einem Linux-basierten Administrationsserver befindet, müssen Sie den POSIX-Pfad angeben. Beispiel: /Pfad/zum/Verzeichnis.

Wenn Sie einen Netzwerkordner auswählen, der sich auf einem Linux-Administrationsserver befindet, müssen Sie vorher durch das Mounten des Ordners sicherstellen, dass von dem Gerät mit installiertem Administrationsserver auf den Netzwerkordner zugegriffen werden kann. Der Zugriff auf den Ordner erfolgt über das SMB-Protokoll.

Diese Option ist standardmäßig deaktiviert.

- **Diff-Dateien herunterladen**

  Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

  Diese Option ist standardmäßig deaktiviert.

- **Updates nach altem Schema herunterladen**

  Ab Version 14 lädt Kaspersky Security Center Linux die Updates von Datenbanken und Softwaremodulen unter Verwendung eines neuen Schemas herunter. Damit die Anwendung die Updates mithilfe des neuen Schemas herunterladen kann, muss die Update-Quelle die Update-Dateien mit den Metadaten enthalten, die mit dem neuen Schema kompatibel sind. Wenn die Update-Quelle die Update-Dateien mit Metadaten enthält, die nur mit dem alten Schema kompatibel sind, aktivieren Sie die Option **Updates nach altem Schema herunterladen**. Andernfalls schlägt die Aufgabe zum Update-Download fehl.

  Sie müssen diese Option beispielsweise aktivieren, wenn als Update-Quelle ein lokaler Ordner oder ein Netzwerkordner angegeben sind, und wenn die Updatedateien in diesem Ordner von einer der folgenden Anwendungen heruntergeladen wurden:

  - Kaspersky Update Utility

    Dieses Tool lädt Updates unter Verwendung des alten Schemas herunter.

  - Kaspersky Security Center 13 Linux

    Beispiel: Ihr Administrationsserver 1 besitzt keine Internetverbindung. In diesem Fall können Sie Updates über einen 2. Administrationsserver herunterladen, welcher über eine Internetverbindung verfügt, und welcher die Updates anschließend in einem lokalen Ordner oder Netzwerkordner ablegt. Dieser dient wiederum als Update-Quelle für den 1. Administrationsserver. Wenn der 2. Administrationsserver mit Version 13 läuft, aktivieren Sie die Option **Updates nach altem Schema herunterladen** in der Aufgabe für den 1. Administrationsserver.

  Diese Option ist standardmäßig deaktiviert.

- **Update-Prüfung ausführen**

  Der Administrationsserver lädt Updates von der Quelle herunter, speichert sie in einer temporären Datenverwaltung und führt die Aufgabe aus, die im Feld **Aufgabe zur Update-Prüfung** angegeben wurde. Wenn die Aufgabe erfolgreich beendet wird, werden die Updates von der temporären Datenverwaltung in einen freigegebenen Ordner auf dem Administrationsserver kopiert und anschließend auf alle Geräte verteilt, für die der Administrationsserver als Update-Quelle dient (Aufgaben mit dem Zeitplantyp **Nach dem Download von Updates in die Datenverwaltung** werden gestartet). Die Aufgabe zum Download von Updates in die Datenverwaltung wird erst nach Abschluss der Aufgabe zur *Update-Prüfung* beendet.

  Diese Option ist standardmäßig deaktiviert.

- **Update-Anforderungsdatei automatisch herunterladen**

  Wenn Sie möchten, dass vom Kaspersky Update Utility nur die erforderlichen Updates in den passenden Konfigurationen heruntergeladen werden, aktivieren Sie diese Option und geben Sie den Pfad an, in den Kaspersky Security Center Linux die Update-Anforderungsdatei mit den Update-Informationen herunterlädt. Die Update-Anforderungsdatei enthält den Zeitstempel und den MD5-Hash zur Versionskontrolle.

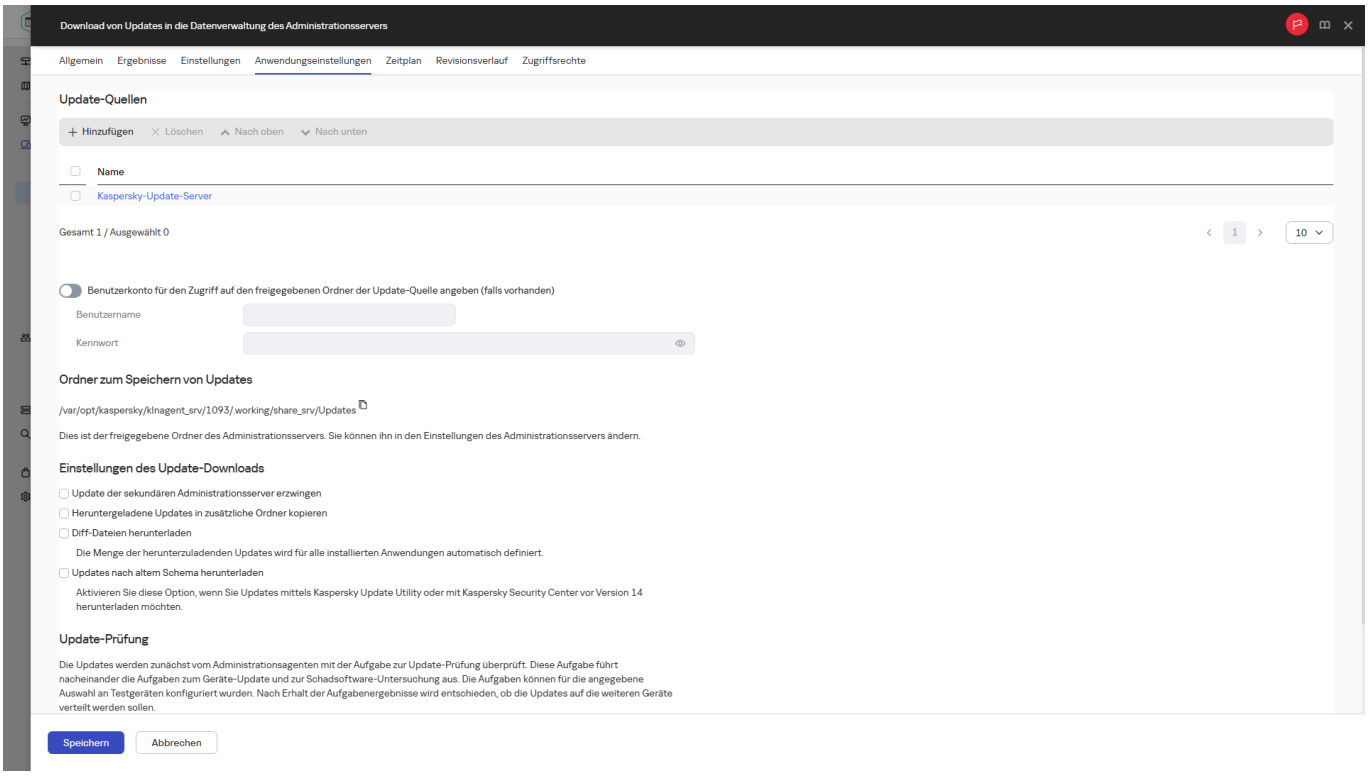
  Stellen Sie sicher, dass die Option **Updates nach altem Schema herunterladen** deaktiviert ist.

  Darüber hinaus muss im Kaspersky Update Utility der Update-Download konfiguriert werden.

  Standardmäßig ist folgender Pfad angegeben: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/retranslation_request.xml. Bei Bedarf können Sie den Standardnamen ("retranslation_request") und den Pfad ändern.

  > Die Anforderungsdatei kann in einem lokalen oder freigegebenen Ordner abgelegt werden. Wenn Sie einen freigegebenen Ordner verwenden, müssen Sie sicherstellen, dass vom Gerät mit installiertem Administrationsserver auf den Ordner zugegriffen werden kann. Wie und mit welchen Tools die Zugriffssicherung umgesetzt wird, ist von Ihrer Infrastruktur abhängig.

  Wenn die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausgeführt wird, erstellt Kaspersky Security Center Linux die Update-Anforderungsdatei im xml-Format in dem von Ihnen angegebenen Ordner. Das Kaspersky Update Utility ruft die Informationen aus der Anforderungsdatei automatisch ab und lädt anschließend nur die erforderlichen Updates herunter. Wenn das Kaspersky Update Utility die Informationen nicht automatisch abrufen kann (z. B. weil das Utility keinen Zugriff auf den Ordner mit der von Kaspersky Security Center Linux erstellten Anforderungsdatei hat), müssen Sie die Datei mithilfe von Drittanbieter-Tools übertragen.



Angeben der Eigenschaften der Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte

9. Erstellen Sie im Fenster mit den Aufgabeneigenschaften auf der Registerkarte **Zeitplan** einen Zeitplan für den Aufgabenstart. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

   - **Aufgabe starten**:

     - **Manuell** (Standardmäßig ausgewählt)

       Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

       Diese Variante ist standardmäßig ausgewählt.

     - **Alle n Minuten**

       Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

       Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

     - **Alle n Stunden**

       Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

       Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

     - **Alle n Tage**

       Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

       Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Monatlich am ausgewählten Tag**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Nach Abschluss einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filter-Symbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- Weitere Aufgabeneinstellungen:

  - **Übersprungene Aufgaben starten**

    Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

    Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Automatische zufällige Verzögerung des Aufgabenstarts innerhalb eines Intervalls von**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

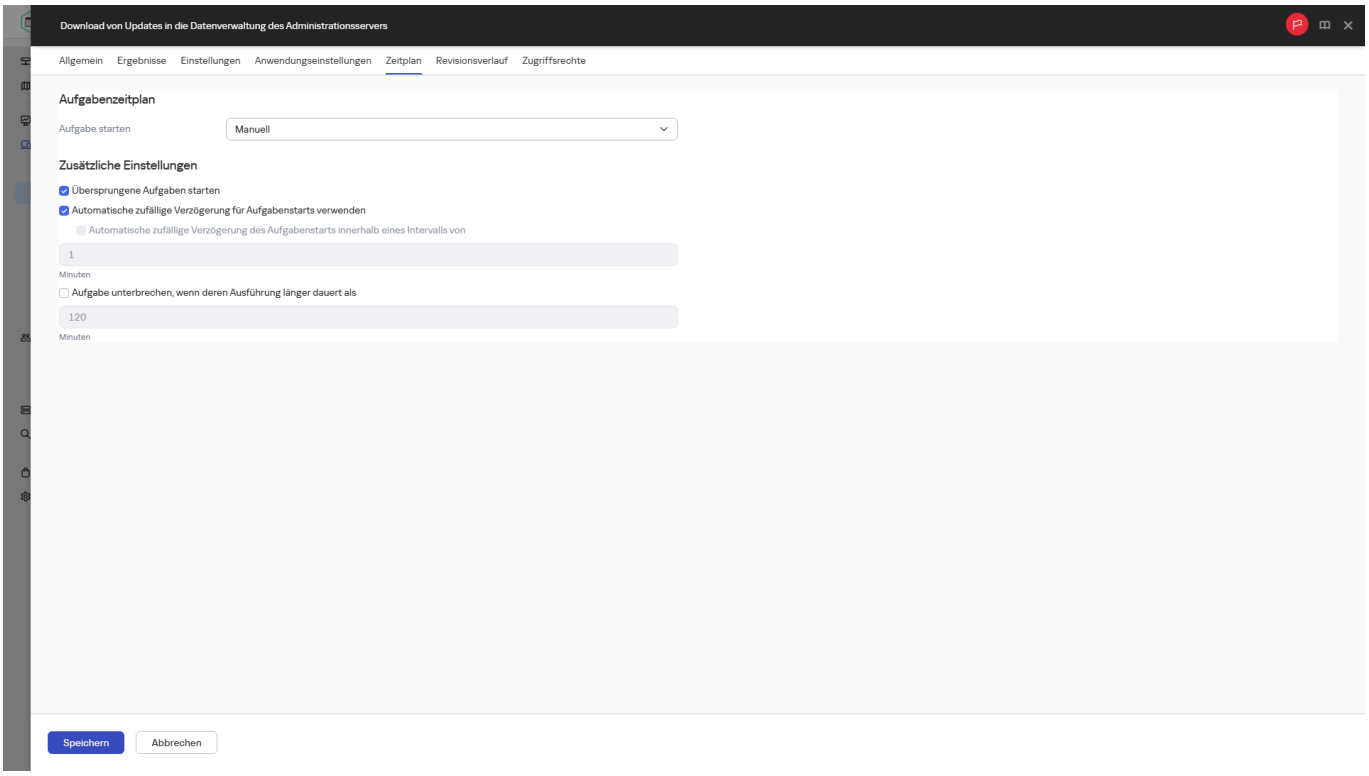
  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

- **Aufgabe unterbrechen, wenn deren Ausführung länger dauert als**

  Nachdem die festlegte Zeitspanne abgelaufen ist, wird die Aufgabe automatisch angehalten, egal ob sie abgeschlossen ist oder nicht.

  Aktivieren Sie diese Option, wenn Sie Aufgaben, deren Ausführung zu lange dauert, unterbrechen (oder anhalten) möchten.

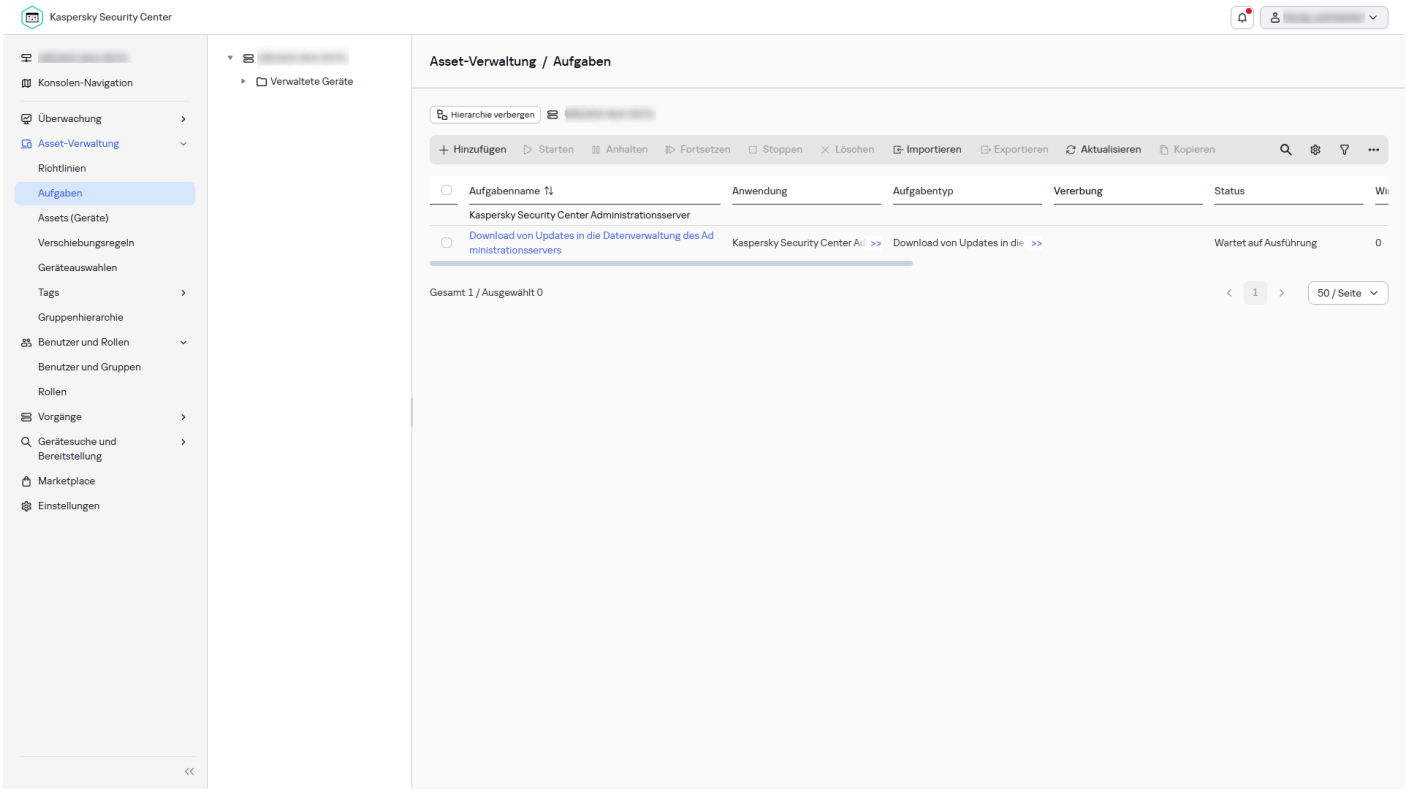
  Diese Option ist standardmäßig deaktiviert. Die Standardzeit für die Aufgabenausführung beträgt 120 Minuten.



Angeben der Zeitplaneinstellungen der Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte

10. Klicken Sie auf die Schaltfläche **Speichern**.

Die Aufgabe wird erstellt und konfiguriert.



Die Aufgabenliste

Nach Fertigstellung der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* werden die Datenbanken-Updates und Updates der Programm-Module von der Update-Quelle geladen und im freigegebenen Ordner des Administrationsservers gespeichert. Wenn die Aufgabe für eine Administrationsgruppe erstellt wird, kommt sie nur auf Administrationsagenten zur Anwendung, die zur angegebenen Administrationsgruppe gehören.

Updates werden aus dem gemeinsamen Ordner des Administrationsservers an Client-Geräte und sekundäre Administrationsserver verteilt.

Heruntergeladene Updates prüfen

Bevor Sie Updates auf den verwalteten Geräten installieren, können Sie die Updates zunächst über die Aufgabe zur *Update-Prüfung* auf Funktionsfähigkeit und Fehler überprüfen. Die Aufgabe zur *Update-Prüfung* wird automatisch im Rahmen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausgeführt. Der Administrationsserver lädt Updates aus der Quelle herunter, speichert sie in einem temporären Verzeichnis und startet die Aufgabe zur *Update-Prüfung*. Wenn die Aufgabe erfolgreich ausgeführt wurde, werden die Updates von der temporären Datenverwaltung in den freigegebenen Ordner des Administrationsservers kopiert. Sie werden an alle Client-Geräte verteilt, für die der Administrationsserver als Update-Quellen dient.

Wenn in den Ergebnissen der Aufgabe zur *Update-Prüfung* die im temporären Verzeichnis liegenden Updates als fehlerhaft eingestuft werden oder wenn die Aufgabe zur *Update-Prüfung* mit einem Fehler beendet wird, werden die Updates nicht im freigegebenen Ordner gespeichert. Auf dem Administrationsserver verbleibt das vorherige Update. Dann werden auch die Aufgaben mit dem Zeitplantyp **Nach dem Download neuer Updates in die Datenverwaltung** nicht gestartet. Diese Vorgänge werden beim nächsten Ausführen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* gestartet, wenn die Prüfung der neuen Updates erfolgreich verläuft.

Das Update gilt als fehlerhaft, wenn mindestens ein Testgerät eine der folgenden Bedingungen erfüllt:

- Es ist ein Fehler in einer Update-Aufgabe aufgetreten.
- Nach Übernahme der Updates hat sich der Status des Echtzeitschutzes der Sicherheitsanwendung geändert.
- Während der Ausführung der Untersuchungsaufgabe auf Befehl wurde ein infiziertes Objekt gefunden.
- Es ist ein Funktionsfehler einer Kaspersky-Anwendung aufgetreten.

Wenn auf keinem Testgerät eine der genannten Bedingungen erfüllt wurde, wird das Set an Updates als ordnungsgemäß anerkannt und die Aufgabe zur *Update-Prüfung* gilt als erfolgreich abgeschlossen.

Bevor Sie mit der Erstellung der Aufgabe zur *Update-Prüfung* beginnen, führen Sie folgende Voraussetzungen aus:

1. Erstellen Sie eine Administrationsgruppe mit mehreren Testgeräten. Sie benötigen diese Gruppe, um die Updates zu prüfen.

   Es wird empfohlen Testgeräte zu verwenden, die gut geschützt sind und die eine Anwendungskonfiguration aufweisen, die im Unternehmensnetzwerk am weitesten verbreitet ist. Dieser Ansatz erhöht während der Untersuchung die Qualität und Wahrscheinlichkeit der Erkennung von Viren und minimiert das Risiko von Fehlalarmen. Wenn Viren auf Testgeräten gefunden werden, wird die Aufgabe zur *Update-Prüfung* als nicht erfolgreich betrachtet.

2. Erstellen Sie die Update-Aufgabe und die Aufgabe zur Schadsoftware-Untersuchung für eine von Kaspersky Security Center Linux unterstütztes Anwendung, z. B. Kaspersky Endpoint Security für Linux. Geben Sie beim Erstellen der Update-Aufgabe und der Aufgabe zur Schadsoftware-Untersuchung die Administrationsgruppe mit den Testgeräten an.

   Die Aufgabe zur *Update-Prüfung* führt die Update-Aufgabe und die Aufgabe zur Schadsoftware-Untersuchung auf den Testgeräten nacheinander aus, um zu überprüfen, ob alle Updates zulässig sind. Beim Erstellen der Aufgabe zur *Update-Prüfung*, müssen Sie zusätzlich die Update-Aufgabe und die Aufgabe zur Schadsoftware-Untersuchung angeben.

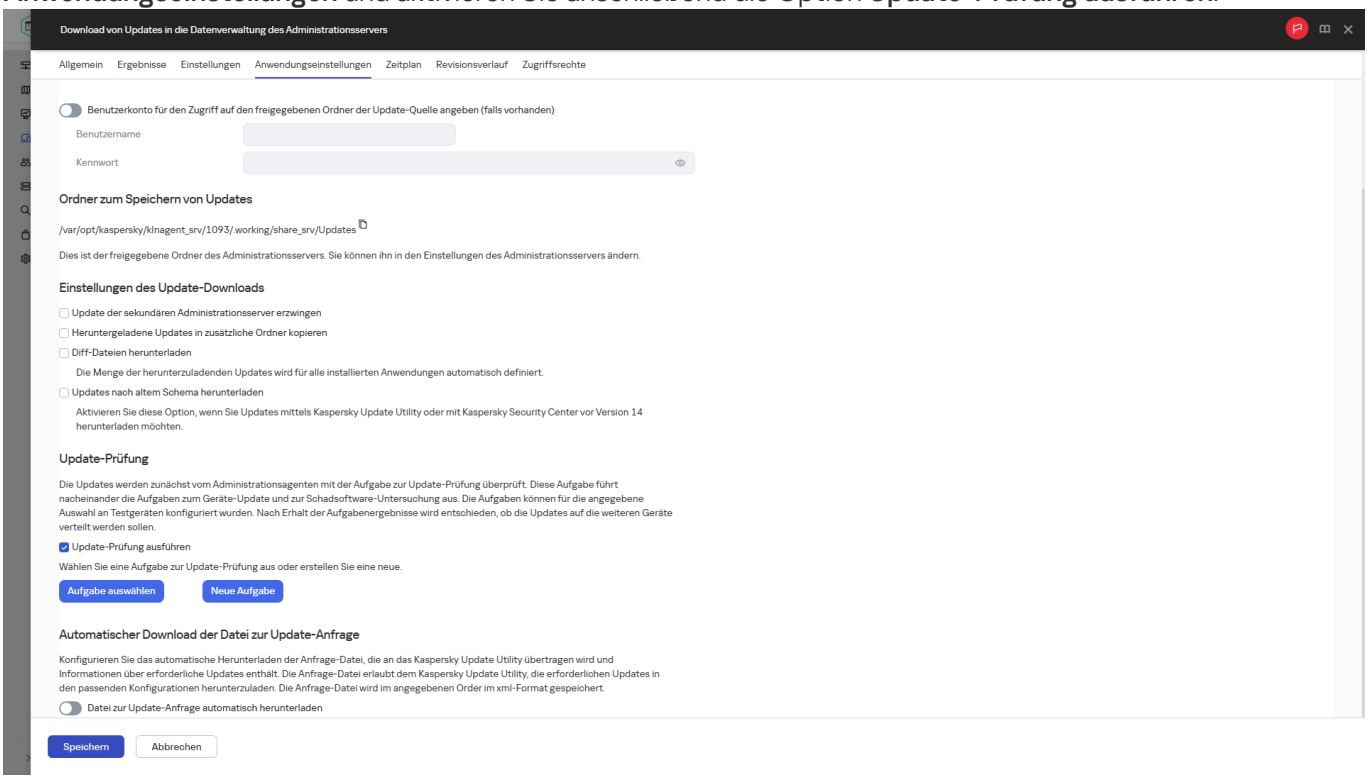
3. Erstellen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*.

Damit Kaspersky Security Center Linux die empfangenen Updates überprüft, bevor sie auf die Client-Geräte verteilt werden:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.

2. Klicken Sie auf die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers**.

3. Wechseln Sie im folgenden Fenster mit den Aufgabeneigenschaften zur Registerkarte **Anwendungseinstellungen** und aktivieren Sie anschließend die Option **Update-Prüfung ausführen**.



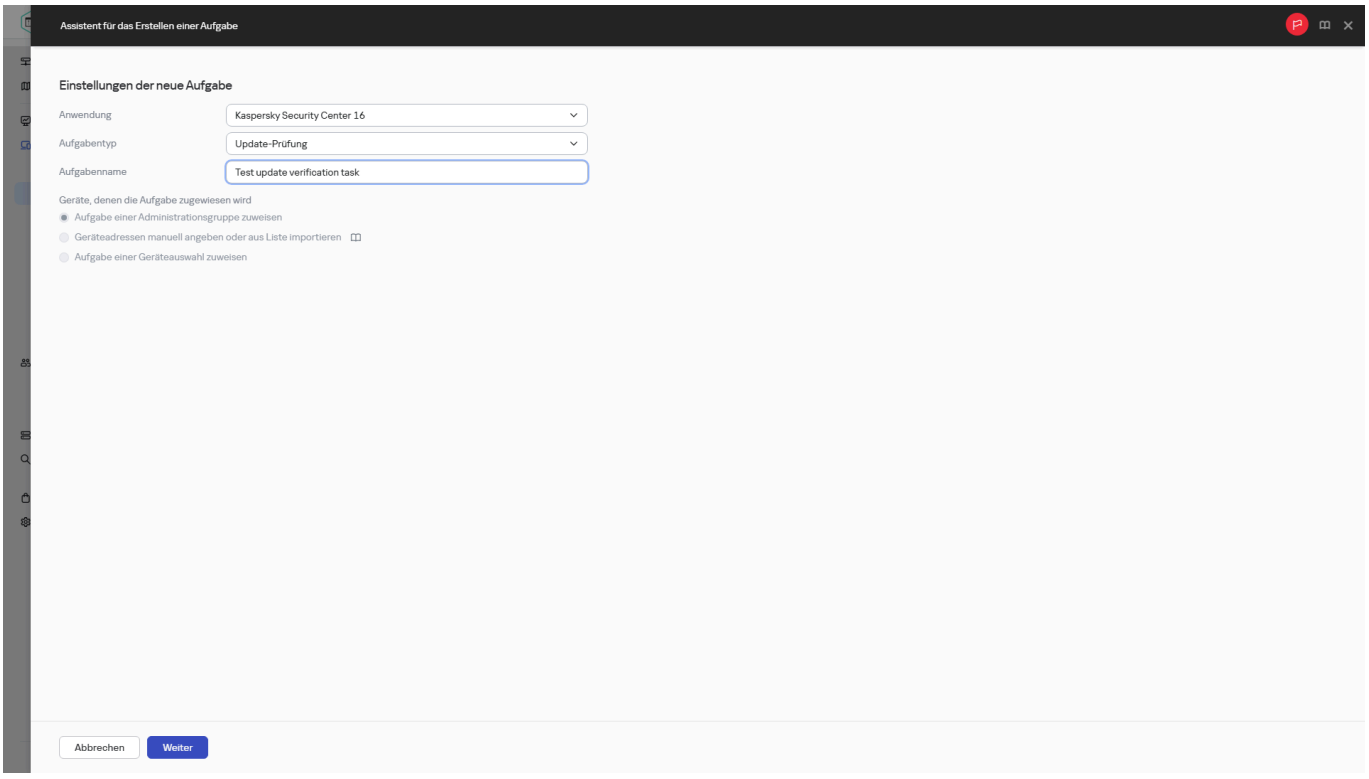
Eigenschaften der Aufgabe Download von Updates in die Datenverwaltung des Administrationsservers

4. Wenn die Aufgabe zur *Update-Prüfung* existiert, klicken Sie auf die Schaltfläche **Aufgabe auswählen**. Wählen Sie im folgenden Fenster die Aufgabe zur *Update-Prüfung* in der Administrationsgruppe mit den Testgeräten aus.

5. Wenn Sie die Aufgabe zur *Update-Prüfung* noch nicht erstellt haben, gehen Sie wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **Neue Aufgabe**.

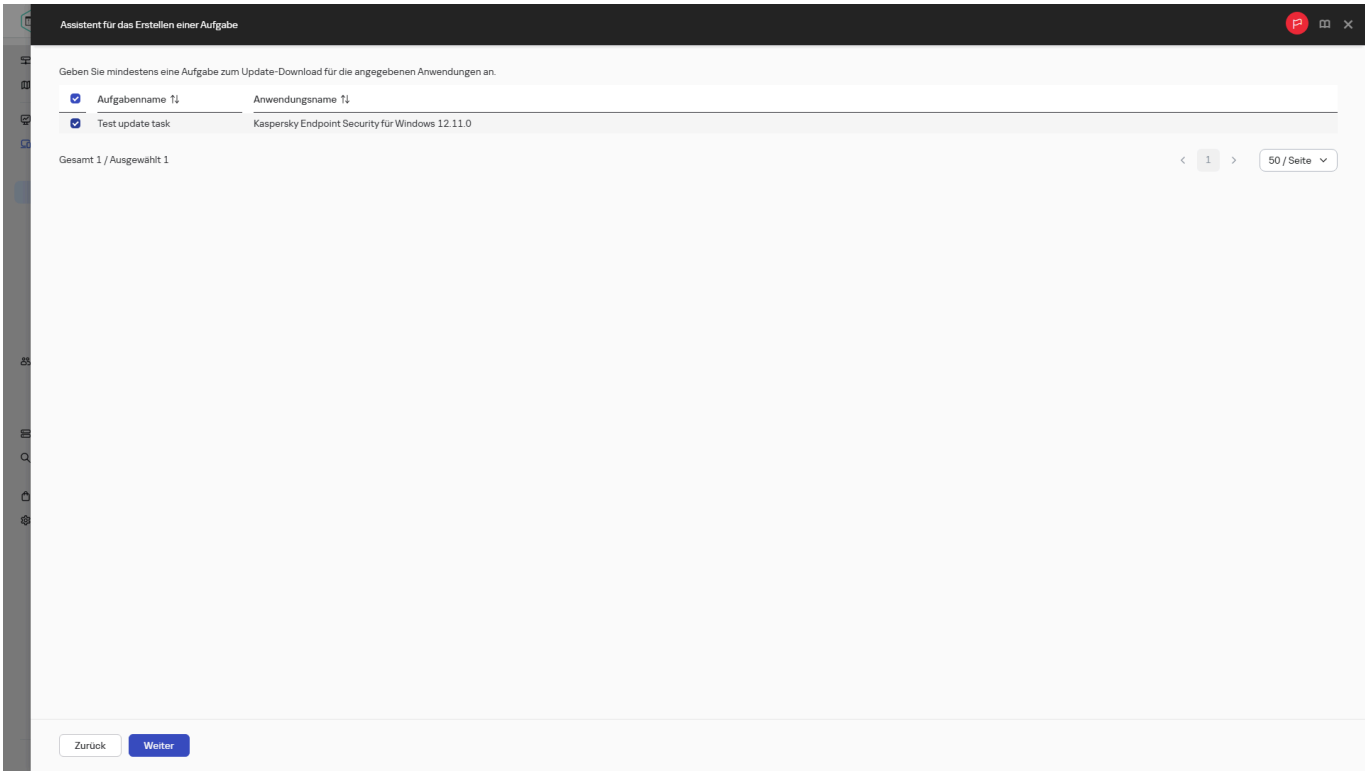
   b. Geben Sie im folgenden Assistenten für das Erstellen einer Aufgabe einen Aufgabennamen an, wenn Sie den voreingestellten Namen ändern möchten.



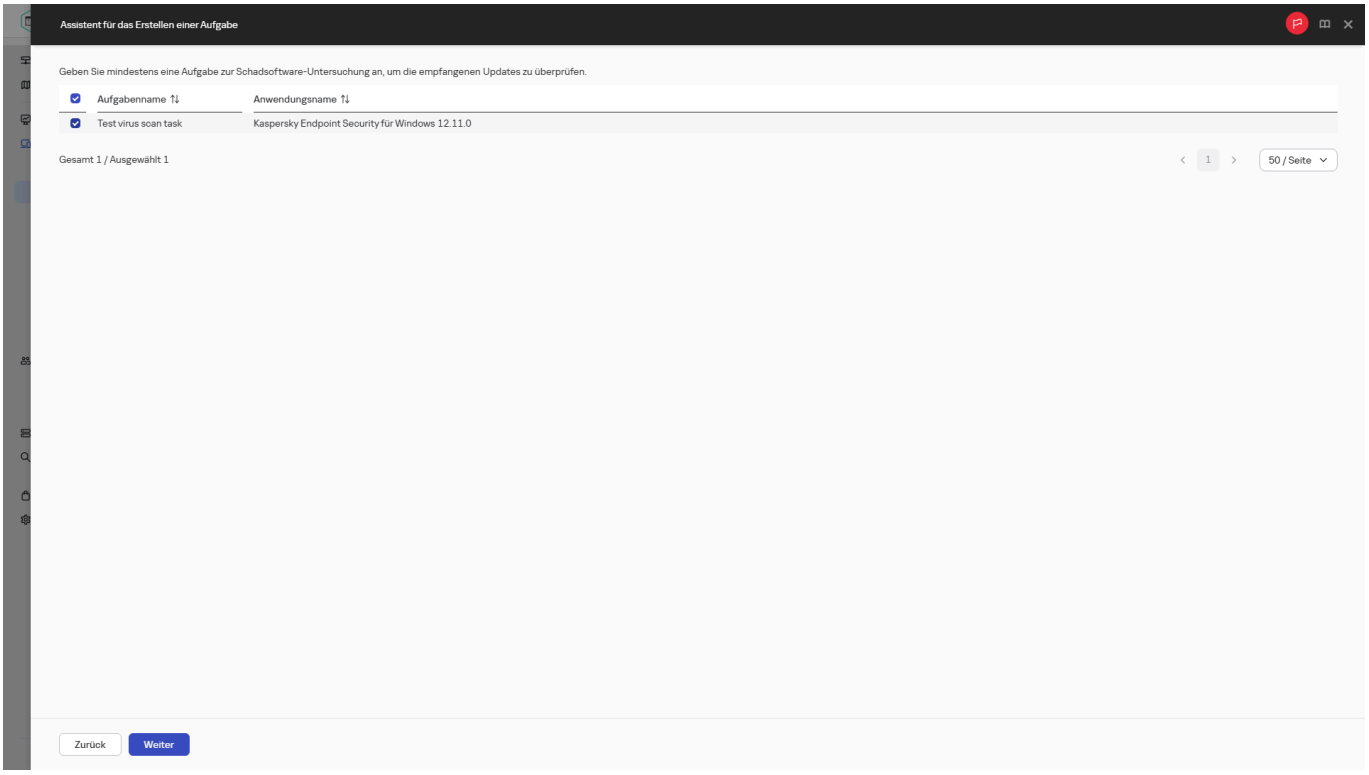
Erstellen einer Aufgabe zur Update-Prüfung

   a. Wählen Sie die zuvor erstellte Administrationsgruppe mit den Testgeräten aus.

   b. Wählen Sie für eine erforderliche Anwendung, die von Kaspersky Security Center Linux unterstützt wird, die Update-Aufgabe aus.



a. Wählen Sie für eine erforderliche Anwendung, die von Kaspersky Security Center Linux unterstützt wird, die Aufgabe zur Schadsoftware-Untersuchung aus.



Auswählen der Aufgabe zur Schadsoftware-Untersuchung

Danach werden die folgenden Optionen angezeigt. Es wird empfohlen, diese aktiviert zu lassen:

- **Gerät nach Datenbanken-Update neu starten**

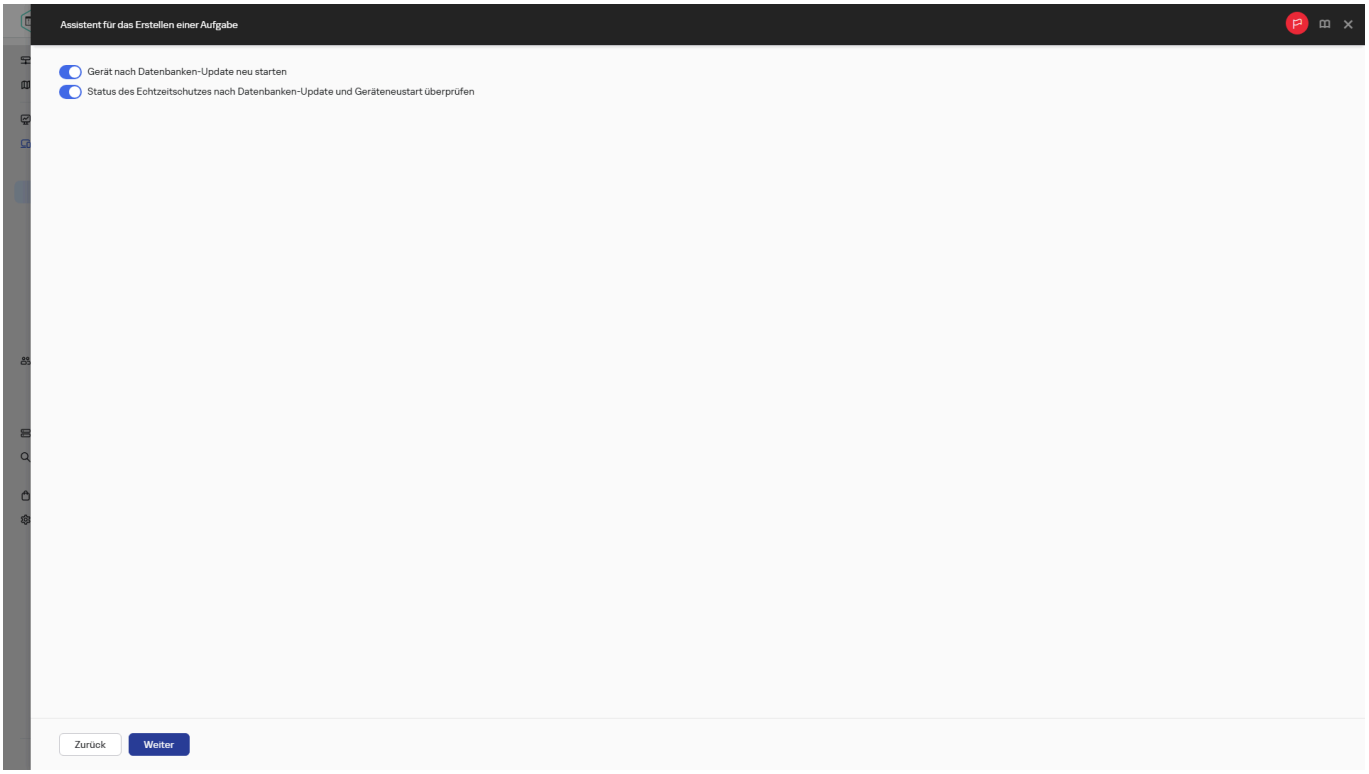
  Nachdem die Antiviren-Datenbanken eines Gerät aktualisiert wurden, wird es empfohlen, das Gerät neu zu starten.

  Die Option ist standardmäßig aktiviert.

- **Status des Echtzeitschutzes nach Datenbanken-Update und Geräteneustart überprüfen**

  Wenn diese Option aktiviert ist prüft die Aufgabe zur *Update-Prüfung*, ob die in die Datenverwaltung des Administrationsservers heruntergeladenen Updates zulässig sind und ob die Schutzstufe nach dem Update der Antiviren-Datenbanken und dem Neustart des Geräts gesunken ist.

Diese Option ist standardmäßig aktiviert.



Angeben der Aufgabeneinstellungen

a. Geben Sie ein Konto an, unter welchem die Aufgabe zur *Update-Prüfung* ausgeführt wird. Sie können Ihr Konto verwenden und die Option **Standardbenutzerkonto** aktiviert lassen. Alternativ können Sie angeben, dass die Aufgabe unter einem anderen Konto ausgeführt werden soll, welches über die erforderlichen Zugriffsrechte verfügt. Wählen Sie dazu die Option **Benutzerkonto festlegen** aus und geben Sie anschließend die Anmeldeinformationen für dieses Konto ein.

6. Klicken Sie auf **Speichern**, um das Eigenschaftenfenster der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* zu schließen.

Die automatische Update-Prüfung ist aktiviert. Wenn Sie jetzt die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ausführen, beginnt diese mit der Update-Prüfung.

Aufgabe zum Download von Updates in die Datenverwaltung der Verteilungspunkte erstellen

Sie können die Aufgabe zum *Download von Updates in die Datenverwaltung der Verteilungspunkte* für eine Administrationsgruppe erstellen. Diese Aufgabe wird für die Verteilungspunkte ausgeführt, die zur angegebenen Administrationsgruppe gehören.

Sie können diese Aufgabe zum Beispiel dann nutzen, wenn der Datenverkehr zwischen dem Administrationsserver und den Verteilungspunkten teurer ist als der Datenverkehr zwischen den Verteilungspunkten und den Kaspersky-Update-Servern, oder wenn Ihr Administrationsserver keinen Internetzugang hat.

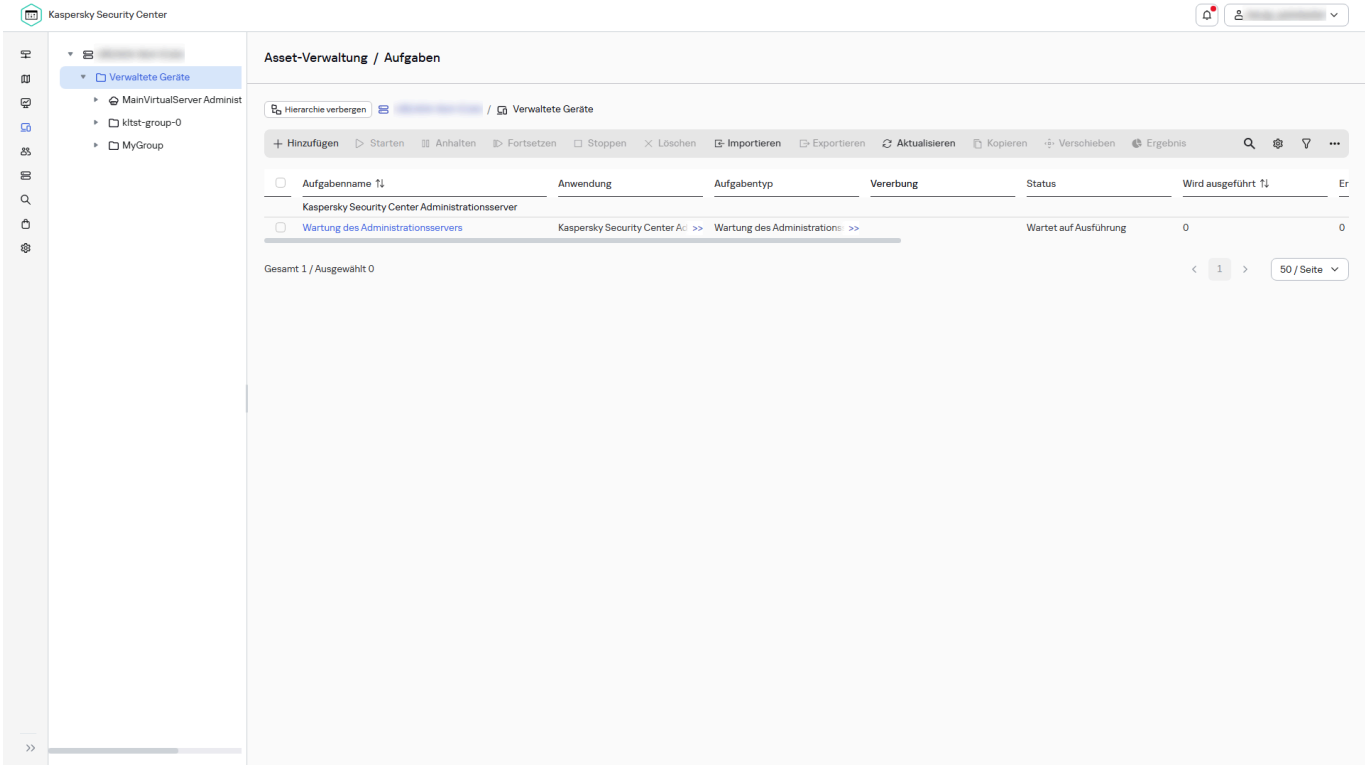
Diese Aufgabe ist erforderlich, um Updates von Kaspersky-Update-Servern in die Datenverwaltung der Verteilungspunkte herunterzuladen. Die Liste der Updates enthält:

- Updates von Datenbanken und Softwaremodulen für Kaspersky-Sicherheitsanwendungen
- Updates der Kaspersky Security Centers-Komponenten
- Updates von Kaspersky-Sicherheitsanwendungen

Nachdem die Updates heruntergeladen wurden, können Sie an die verwalteten Geräte weitergegeben werden.

*So erstellen Sie die Aufgabe **Updates in die Datenverwaltung der Verteilungspunkte herunterladen** für eine ausgewählte Administrationsgruppe:*

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.



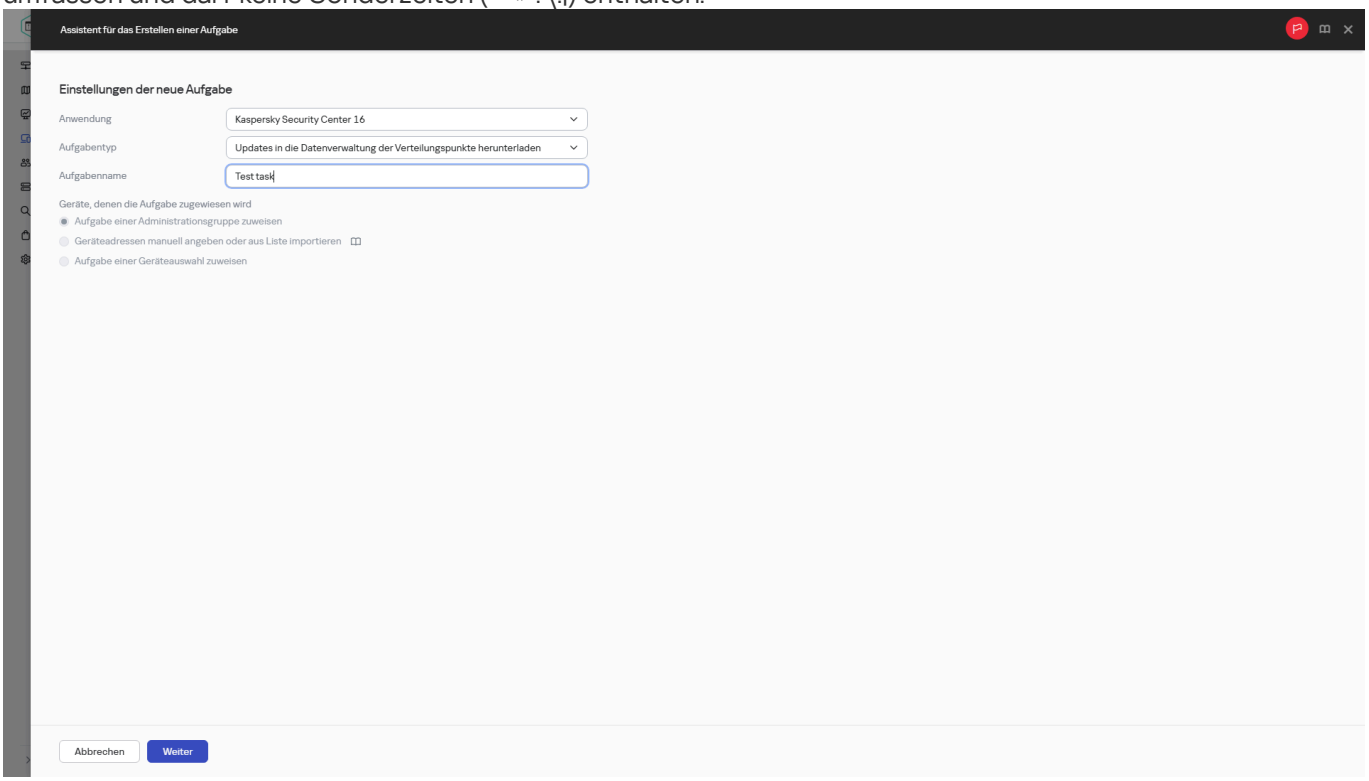
Der Abschnitt Aufgaben

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.

3. Wählen Sie für Kaspersky Security Center im Feld **Aufgabentyp** die Option **Updates in die Datenverwaltung der Verteilungspunkte herunterladen**.

4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.



Aufgabe zum Updates in die Datenverwaltung der Verteilungspunkte herunterladen erstellen

5. Wählen Sie eine Optionsschaltfläche, um die Administrationsgruppe, die Geräteauswahl oder die Geräte, für die Aufgabe gilt, festzulegen.

6. Wenn Sie im Schritt **Erstellung der Aufgabe abschließen** die Standardeinstellungen der Aufgabe ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

7. Klicken Sie auf **Erstellen**.

   Die Aufgabe wird erstellt und in der Aufgabenliste angezeigt.

8. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

9. Geben Sie auf der Registerkarte **Anwendungseinstellungen** im Fenster der Aufgabeneigenschaften die folgenden Einstellungen an:

   - **Update-Quellen**

     Als Update-Quelle für den Verteilungspunkt können die folgenden Ressourcen verwendet werden:

     - Kaspersky-Update-Server

       HTTP(S)-Server bei Kaspersky, von denen Kaspersky-Anwendungen Updates für Datenbanken und Anwendungsmodule herunterladen.

       Diese Variante ist standardmäßig festgelegt.

     - Lokaler Ordner oder Netzwerkordner

       Lokaler oder Netzwerkordner, der die neuesten Updates enthält. Als Netzwerkordner kann nur eine eingebundene SMB-Freigabe verwendet werden. Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben.

In der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und der Aufgabe *Download von Updates in die Datenverwaltung der Verteilungspunkte* funktioniert die Benutzerauthentifizierung nicht, wenn Sie einen kennwortgeschützten lokalen Ordner oder Netzwerkordner als Update-Quelle auswählen. Um dieses Problem zu beheben, stellen Sie zuerst den kennwortgeschützten Ordner bereit und geben Sie dann die erforderlichen Anmeldedaten an, z. B. über das Betriebssystem. Danach können Sie diesen Ordner als Update-Quelle in einer Aufgabe für Update-Downloads auswählen. Für Kaspersky Security Center Linux müssen Sie keine Anmeldedaten eingeben.

- **Ordner zum Speichern von Updates**

  Der Pfad zum angegebenen Ordner, in dem die bezogenen Updates gespeichert werden. Sie können den Pfad des angegebenen Ordners in die Zwischenablage kopieren. Für eine Gruppenaufgabe können Sie den Pfad eines angegebenen Ordners nicht ändern.

- **Diff-Dateien herunterladen**

  Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

  Diese Option ist standardmäßig deaktiviert.

- **Updates nach altem Schema herunterladen**

  Ab Version 14 lädt Kaspersky Security Center Linux die Updates von Datenbanken und Softwaremodulen unter Verwendung eines neuen Schemas herunter. Damit die Anwendung die Updates mithilfe des neuen Schemas herunterladen kann, muss die Update-Quelle die Update-Dateien mit den Metadaten enthalten, die mit dem neuen Schema kompatibel sind. Wenn die Update-Quelle die Update-Dateien mit Metadaten enthält, die nur mit dem alten Schema kompatibel sind, aktivieren Sie die Option **Updates nach altem Schema herunterladen**. Andernfalls schlägt die Aufgabe zum Update-Download fehl.

  Sie müssen diese Option beispielsweise aktivieren, wenn als Update-Quelle ein lokaler Ordner oder ein Netzwerkordner angegeben sind, und wenn die Updatedateien in diesem Ordner von einer der folgenden Anwendungen heruntergeladen wurden:

  - Kaspersky Update Utility

    Dieses Tool lädt Updates unter Verwendung des alten Schemas herunter.

  - Kaspersky Security Center 13 Linux

    Ein Verteilungspunkt kann beispielsweise so konfiguriert sein, dass er die Updates aus einem lokalen oder aus einem Netzwerkordner übernimmt. In diesem Fall können Sie Updates über einen Administrationsserver mit Internetverbindung herunterladen und die Updates anschließend im lokalen Ordner des Verteilungspunkts ablegen. Wenn der Administrationsserver in Version 13 ausgeführt wird, aktivieren Sie in der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* die Option **Updates nach altem Schema herunterladen**.

  Diese Option ist standardmäßig deaktiviert.

10. Erstellen Sie einen Zeitplan für den Aufgabenstart. Geben Sie erforderlichenfalls die folgenden Einstellungen an:

- **Aufgabe starten**:

  - **Manuell** (Standardmäßig ausgewählt)

    Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

    Diese Variante ist standardmäßig ausgewählt.

- **Alle n Minuten**

  Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

  Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

- **Alle n Stunden**

  Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

  Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

- **Alle n Tage**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

  Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

- **Nach Wochentagen**

  Die Aufgabe wird regelmäßig an den festgelegten Wochentagen zur festgelegten Uhrzeit ausgeführt.

  Die Aufgabe wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **Monatlich am ausgewählten Tag**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Abschluss einer anderen Aufgabe**

  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

  Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

  - Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
  - Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

    Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
  - Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.

- **Übersprungene Aufgaben starten**

  Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

  Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

  Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Automatische zufällige Verzögerung des Aufgabenstarts innerhalb eines Intervalls von**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

11. Klicken Sie auf die Schaltfläche **Speichern**.

    Die Aufgabe wird erstellt und konfiguriert.

    Zusätzlich zu den Einstellungen, die Sie während der Aufgabenerstellung festlegen, können Sie andere Eigenschaften einer erstellten Aufgabe ändern.

Bei der Ausführung der Aufgabe *Updates in die Datenverwaltung der Verteilungspunkte herunterladen* werden die Datenbanken-Updates und Updates der Programm-Module aus der Update-Quelle heruntergeladen und im freigegebenen Ordner gespeichert. Die heruntergeladenen Updates werden nur von jenen Verteilungspunkten verwendet, die zur angegebenen Administrationsgruppe gehören und für die keine separate Aufgabe zum Update-Download festgelegt wurde.

Die Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers weitere Update-Quellen hinzufügen

Wenn Sie die Aufgabe zum Download von Updates in die Datenverwaltung des Administrationsservers erstellen oder verwenden, stehen die folgenden Update-Quellen zur Auswahl:

- Kaspersky-Update-Server
- Primärer Administrationsserver

  Diese Ressource gilt für Aufgaben, die für einen sekundären oder virtuellen Administrationsserver erstellt wurden.

- Lokaler Ordner oder Netzwerkordner

  In der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* und der Aufgabe *Download von Updates in die Datenverwaltung der Verteilungspunkte* funktioniert die Benutzerauthentifizierung nicht, wenn Sie einen kennwortgeschützten lokalen Ordner oder Netzwerkordner als Update-Quelle auswählen. Um dieses Problem zu beheben, stellen Sie zuerst den kennwortgeschützten Ordner bereit und geben Sie dann die erforderlichen Anmeldedaten an, z. B. über das Betriebssystem. Danach können Sie diesen Ordner als Update-Quelle in einer Aufgabe für Update-Downloads auswählen. Für Kaspersky Security Center Linux müssen Sie keine Anmeldedaten eingeben.

Die Kaspersky-Update-Server werden standardmäßig verwendet, Sie können die Updates jedoch auch aus einem lokalen Ordner oder Netzwerkordner herunterladen. Den Ordner können Sie beispielsweise verwenden, wenn Ihr Netzwerk keinen Internetzugriff hat. In diesem Fall können Sie die Updates manuell von den Kaspersky-Update-Servern herunterladen und die heruntergeladenen Dateien im erforderlichen Ordner ablegen. Sie können nur einen Pfad für einen lokalen Ordner oder Netzwerkordner angeben.

Bei Auswahl eines lokalen Ordners ist es erforderlich, einen Ordner auf dem Gerät mit dem installierten Administrationsserver anzugeben. Der Pfad des Ordners hängt vom Betriebssystem auf dem Gerät ab. Da sich der lokale Ordner auf einem Linux-basierten Administrationsserver befindet, müssen Sie den POSIX-Pfad angeben. Beispiel: /Pfad/zum/Verzeichnis.

Als Netzwerkordner kann nur eine eingebundene SMB-Freigabe verwendet werden. Wenn für die SMB-Freigabe eine Authentifizierung erforderlich ist, muss diese zuvor mit den erforderlichen Anmeldeinformationen im System eingebunden werden. Es wird davon abgeraten, das SMB1-Protokoll zu verwenden, da es unsicher ist.

So fügen Sie Update-Quellen hinzu:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Download von Updates in die Datenverwaltung des Administrationsservers**.
3. Gehen Sie zur Registerkarte **Anwendungseinstellungen**.
4. Klicken Sie in der Tabelle **Update-Quellen** auf die Schaltfläche **Hinzufügen**.
5. Fügen Sie im neuen Fenster die gewünschten Quellen hinzu und klicken Sie anschließend auf die Schaltfläche **Speichern**.

   Wenn Sie das Kontrollkästchen **Lokaler Ordner oder Netzwerkordner** aktivieren, geben Sie einen Ordnerpfad an.
6. Klicken Sie im Aufgabenfenster auf **Speichern**.

   Jetzt werden Updates aus den angegebenen Quellen in die Datenverwaltung des Administrationsservers heruntergeladen.

Wenn Sie sowohl die Kaspersky-Update-Server als auch einen lokalen Ordner oder einen Netzwerkordner hinzufügen, können Sie für die Updates Prioritäten festlegen. Aktivieren Sie dazu in der Tabelle **Update-Quellen** das Kontrollkästchen neben dem Update, dessen Priorität Sie ändern möchten, und klicken Sie anschließend auf die Schaltfläche **Nach oben** oder **Nach unten**.

Genehmigen und Ablehnen von Software-Updates

Die Einstellungen einer Aufgabe zur Update-Installation erfordern eventuell die Genehmigung der zu installierenden Updates. Sie können Updates, die installiert werden müssen, genehmigen und Updates, die nicht installiert werden dürfen, ablehnen.

Beispielsweise können Sie die Update-Installation zuerst in einer Testumgebung überprüfen und sich vergewissern, dass sie den Betrieb der Geräte nicht stören, und erst anschließend die Installation dieser Updates auf Client-Geräten zulassen.

Das Genehmigen und Ablehnen von Updates ist nur für Administrationsagenten und verwaltete Anwendungen verfügbar, die auf Windows-basierten Client-Geräten installiert sind. Ein nahtloses Update der folgenden Komponenten wird nicht unterstützt: Administrationsserver, Kaspersky Security Center Web Console und Web-Plug-ins zur Verwaltung. Um diese Komponenten zu aktualisieren, müssen Sie die jeweils aktuellste Version von der Kaspersky-Website herunterladen und anschließend manuell installieren.

So genehmigen Sie ein oder mehrere Updates oder lehnen die Updates ab:

1. Gehen Sie im Hauptmenü zu **Software-Verwaltung → Kaspersky-Anwendungen → Nahtlose Updates**.

   Eine Liste der verfügbaren Updates wird geöffnet.

Für Updates von verwalteten Anwendungen muss möglicherweise eine bestimmte Mindestversion von Kaspersky Security Center installiert sein. Wenn diese Version höher ist als Ihre aktuelle Version, werden diese Updates zwar angezeigt, können jedoch nicht genehmigt werden. Außerdem können aus solchen Updates keine Installationspakete erstellt werden, bevor Kaspersky Security Center nicht aktualisiert wurde. Sie werden aufgefordert, Ihre Kaspersky Security Center-Instanz auf die erforderliche Mindestversion zu aktualisieren.

2. Akzeptieren Sie gegebenenfalls die EULA, indem Sie auf **Lizenzverträge anzeigen und akzeptieren** klicken.
3. Wählen Sie die Updates aus, die Sie genehmigen oder ablehnen möchten.
4. Klicken Sie auf **Genehmigen**, um die ausgewählten Updates zu genehmigen, oder auf **Ablehnen**, um die ausgewählten Updates abzulehnen.

   Der Standardwert ist *Nicht festgestellt*.

Die Updates, für die Sie den Status *Genehmigt* auswählen, werden in eine Warteschlange für die Installation verschoben.

Die Updates, für die Sie den Status *Abgelehnt* auswählen, werden von allen Geräten, auf denen sie bisher installiert waren, deinstalliert (falls möglich). Ferner werden sie in Zukunft nicht auf anderen Geräten installiert.

Einige Updates für Kaspersky-Anwendungen können nicht deinstalliert werden. Wenn Sie für diese den Status *Abgelehnt* festlegen, deinstalliert Kaspersky Security Center Linux diese Updates nicht von den Geräten, auf denen sie bereits installiert sind. Diese Updates werden jedoch in Zukunft nicht mehr auf anderen Geräten installiert.

Wenn Sie an Updates für Drittanbieter-Programme den Status *Abgelehnt* vergeben, werden diese Updates nicht auf jenen Geräten installiert, auf denen eine Installation vorgesehen war, aber noch nicht durchgeführt wurde. Auf den Geräten, auf denen die Updates bereits installiert sind, werden diese beibehalten. Wenn Sie solche Updates löschen müssen, können Sie dies lokal und manuell tun.

Automatische Installation von Updates für Kaspersky Endpoint Security für Windows

Sie können das automatische Update für die Datenbanken und Programm-Module von Kaspersky Endpoint Security für Windows auf Client-Geräten konfigurieren.

So konfigurieren Sie den Download und die automatische Installation von Updates für Kaspersky Endpoint Security für Windows auf Geräten:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie für Kaspersky Endpoint Security für Windows die Variante **Update** als Untertyp der Aufgabe aus.

4. Geben Sie den Namen der Aufgabe an, die Sie erstellen. Der Aufgabenname darf höchstens 100 Zeichen lang sein und darf keine Sonderzeichen ("*<>?\:|) enthalten.

5. Wählen Sie den Aufgabenbereich aus.

6. Geben Sie die Administrationsgruppe, die Geräteauswahl oder die Geräte an, für welche die Aufgabe gilt.

7. Wenn Sie beim Schritt **Erstellung der Aufgabe abschließen** die Standardeinstellungen der Aufgabe ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

8. Klicken Sie auf **Erstellen**.

   Die Aufgabe wird erstellt und in der Aufgabenliste angezeigt.

9. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.

10. Legen Sie auf der Registerkarte **Anwendungseinstellungen** im Fenster mit den Aufgabeneigenschaften die Einstellungen der Update-Aufgabe für den lokalen oder mobilen Modus fest:

    - **Lokaler Modus**: Zwischen dem Gerät und Administrationsserver besteht eine Verbindung.

    - **Mobiler Modus**: Zwischen Kaspersky Security Center Linux und dem Gerät besteht keine Verbindung (beispielsweise, wenn das Gerät nicht mit dem Internet verbunden ist).

11. Aktivieren Sie die Update-Quellen, die Sie zur Aktualisierung der Datenbanken und Programm-Module von Kaspersky Endpoint Security für Windows verwenden möchten. Bei Bedarf können Sie die Position der Quellen in der Liste ändern. Dafür gibt es die Schaltflächen **Nach oben** und **Nach unten**. Wenn mehrere Update-Quellen aktiviert sind, versucht Kaspersky Endpoint Security für Windows, sich anhand der Liste mit einer Quelle zu verbinden. Die Update-Aufgabe wird ausgeführt, indem das Update-Paket von der ersten verfügbaren Quelle abgerufen wird.

12. Aktivieren Sie die Option **Genehmigte Updates für Anwendungsmodule installieren**, um die Updates für Programm-Module zusammen mit den Programm-Datenbanken herunterzuladen und zu installieren.

    Wenn diese Option aktiviert ist, benachrichtigt Kaspersky Endpoint Security für Windows den Benutzer über verfügbare Updates für Programm-Module und nimmt bei der Update-Aufgabe die Updates für Programm-Module in das Update-Paket auf. Kaspersky Endpoint Security für Windows installiert nur die Updates, für die Sie den Status *Genehmigt* festgelegt haben. Sie werden lokal über die Programmoberfläche oder über Kaspersky Security Center Linux installiert.

    Sie können auch die Option **Kritische Updates für Anwendungsmodule automatisch installieren** aktivieren. Wenn Updates für Programm-Module verfügbar sind, installiert Kaspersky Endpoint Security für Windows automatisch alle Updates mit dem Status *Kritisch*. Die restlichen Updates werden installiert, nachdem Sie diese genehmigt haben.

    Wenn es für ein Update der Programm-Module erforderlich ist, dass der Benutzer die Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie liest und akzeptiert, werden die Updates erst installiert, nachdem der Benutzer die Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie akzeptiert hat.

13. Aktivieren Sie das Kontrollkästchen **Updates in Ordner kopieren**, damit die Anwendung die heruntergeladenen Updates in einen Ordner kopiert, und geben Sie dann den Pfad an.

14. Planen Sie die Aufgabe. Um zeitnahe Updates sicherzustellen, wird empfohlen, die Option **Nach dem Download von Updates in die Datenverwaltung** zu aktivieren.

15. Klicken Sie auf **Speichern**.

Beim Ausführen der Aufgabe **Update** sendet die Anwendung Anfragen an die Kaspersky-Update-Server.

Einige Updates erfordern die Installation der neuesten Versionen von Verwaltungs-Plug-ins.

Über die Verwendung von Diff-Dateien zum Update von Kaspersky-Datenbanken und Software-Modulen

Beim Update-Download von den Kaspersky-Update-Servern optimiert Kaspersky Security Center Linux den Datenverkehr durch die Verwendung von Diff-Dateien. Sie können festlegen, dass Geräte (Administrationsserver, Verteilungspunkte, Client-Geräte), die Updates von anderen Geräten in Ihrem Netzwerk erhalten, ebenfalls Diff-Dateien verwenden.

Über die Funktion zum Download von Diff-Dateien

Eine Diff-Datei beschreibt den Unterschied zwischen zwei Versionen der Datei einer Datenbank oder eines Programm-Moduls. Die Verwendung von Diff-Dateien entlastet den Datenverkehr in Ihrem Unternehmensnetzwerk, da Diff-Dateien weniger Platz einnehmen als die vollständigen Dateien der Datenbanken und Software-Module. Wenn die Funktion *Diff-Dateien herunterladen* auf dem Administrationsserver oder dem Verteilungspunkt aktiviert ist, werden die Diff-Dateien auf diesem Administrationsserver oder Verteilungspunkt gespeichert. So können Geräte, die Updates vom Administrationsserver oder einem Verteilungspunkt erhalten, die gespeicherten Diff-Dateien verwenden, um ihre Datenbanken und Software-Module zu aktualisieren.

Um die Verwendung von Diff-Dateien zu optimieren, wird empfohlen, den Update-Zeitplan der Geräte mit dem Update-Zeitplan des Administrationsservers oder dem Verteilungspunkt, von denen sie ihre Updates erhalten, zu synchronisieren. Der Datenverkehr kann jedoch auch dann reduziert werden, wenn die Geräte viel seltener aktualisiert werden als der Administrationsserver oder der Verteilungspunkt, von dem sie ihre Updates erhalten.

Verteilungspunkte verwenden kein IP-Multicast zur automatischen Verteilung von Diff-Dateien.

Funktion zum Herunterladen von Diff-Dateien aktivieren

Schritte

1. **Aktivieren der Funktion auf dem Administrationsserver**

   Aktivieren Sie die Funktion in den Einstellungen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*.

2. **Aktivieren der Funktion für einen Verteilungspunkt**

   Aktivieren Sie die Funktion für Verteilungspunkte, die Updates mithilfe der Aufgabe *Download von Updates in die Datenverwaltung der Verteilungspunkte* erhalten.

Aktivieren Sie anschließend in den Einstellungen der Richtlinie des Administrationsagenten die Funktion für die Verteilungspunkte, die Updates vom Administrationsserver erhalten.

Aktivieren Sie anschließend die Funktion für Verteilungspunkte, die Updates vom Administrationsserver erhalten.

Die Funktion wird in den Einstellungen des Administrationsagenten und – falls die Verteilungspunkte manuell zugewiesen werden und Sie die Einstellungen der Richtlinie umgehen möchten – im Abschnitt **Verteilungspunkte** in den Eigenschaften des Administrationsservers aktiviert.

Um zu prüfen, ob die Funktion zum Download von Diff-Dateien erfolgreich aktiviert wurde, können Sie den internen Datenverkehr vor und nach der Implementierung des Szenarios messen.

Updates mittels Verteilungspunkten herunterladen

In Kaspersky Security Center Linux können die Verteilungspunkte Updates vom Administrationsserver, von den Servern von Kaspersky, aus lokalen oder Netzwerkordnern abrufen.

Um den Update-Download für den Verteilungspunkt anzupassen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verteilungspunkte** aus.

3. Klicken Sie auf den Namen des Verteilungspunkts, über den Updates an die Client-Geräte in der Gruppe verteilt werden.

4. Wählen Sie im Eigenschaftenfenster des Verteilungspunkts den Abschnitt **Update-Quelle** aus.

5. Wählen Sie die Update-Quelle für den Verteilungspunkt:

   - **Update-Quelle**

     Wählen Sie eine Update-Quelle für den Verteilungspunkt aus:

     - Damit der Verteilungspunkt die Updates vom Administrationsserver erhält, wählen Sie **Vom Administrationsserver beziehen**.

     - Damit Verteilungspunkte Updates anhand einer Aufgabe beziehen können, wählen Sie **Aufgabe zum Update-Download verwenden** aus und geben Sie anschließend eine Aufgabe vom Typ *Download von Updates in die Datenverwaltung der Verteilungspunkte* an:

       - Wenn eine solche Aufgabe bereits auf dem Gerät vorhanden ist, wählen Sie die Aufgabe in der Liste aus.

       - Wenn auf dem Gerät noch keine derartige Aufgabe vorhanden ist, klicken Sie auf den Link **Aufgabe erstellen**, um eine Aufgabe zu erstellen. Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Anweisungen des Assistenten.

   - **Diff-Dateien herunterladen**

     Diese Option aktiviert die Funktion zum Download von Diff-Dateien.

     Diese Option ist standardmäßig aktiviert.

Daraufhin bezieht der Verteilungspunkt die Updates von der angegebenen Quelle.

Datenbanken und Software-Module von Kaspersky auf autonomen Geräten aktualisieren

Das Durchführen von Updates der Kaspersky-Datenbanken und Programm-Module auf verwalteten Geräten ist eine wichtige Aufgabe, um den Schutz gegen Viren und andere Bedrohungen aufrechtzuerhalten. In der Regel konfigurieren Administratoren regelmäßige Updates durch die Nutzung der Datenverwaltungen des Administrationsservers.

Wenn Sie Updates von Datenbanken und Programm-Modulen auf einem Gerät (oder auf einer Gruppe von Geräten) durchführen müssen, die nicht mit dem Administrationsserver (primär oder sekundär), einem Verteilungspunkt oder dem Internet verbunden sind, müssen Sie eine alternative Update-Quelle, wie einen FTP-Server oder einen lokalen Ordner, nutzen. In diesem Fall müssen Sie die für die Updates benötigten Dateien über ein Massenspeichergerät, wie beispielsweise ein USB-Stick oder eine externe Festplatte, bereitstellen.

Kopieren Sie die benötigten Updates vom:

- Administrationsserver.

  Um sicherzustellen, dass die Datenverwaltung des Administrationsservers über die, von der auf dem autonomen Gerät installierten Sicherheitsanwendung benötigten, Updates verfügt, muss auf mindestens einem der verwalteten Online-Geräte die gleiche Sicherheitsanwendung installiert sein. Diese Anwendung muss so angepasst sein, dass es mithilfe der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* die Updates aus der Administrationsserver-Datenverwaltung erhält.

- Jedes Gerät, dass die gleiche Sicherheitsanwendung installiert und so konfiguriert hat, dass sie Updates aus den Datenverwaltungen des Administrationsservers oder der Verteilungspunkte, oder direkt von den Kaspersky-Servern erhält.

Unten befindet sich ein Beispiel zur Update-Konfiguration von Datenbanken und Programm-Modulen, in welcher die Updates aus der Datenverwaltung des Administrationsservers kopiert werden.

So aktualisieren Sie Kaspersky-Datenbanken und Programm-Module auf autonomen Geräten:

1. Verbinden Sie einen Wechseldatenträger mit dem Gerät, auf dem der Administrationsserver installiert ist.

2. Kopieren Sie die Update-Dateien auf den Wechseldatenträger.

   Standardmäßig befinden sich die Updates unter:
   /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   Alternativ können Sie Kaspersky Security Center Linux so konfigurieren, dass es die Updates regelmäßig in einen von Ihnen gewählten Ordner kopiert. Verwenden Sie dazu die Option **Heruntergeladene Updates in zusätzliche Ordner kopieren** in den Eigenschaften der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers*. Wenn Sie einen Ordner auf einem USB-Stick oder einer externen Festplatte als Zielordner für diese Option angeben, wird dieses Massenspeichergerät stets über die aktuellsten Versionen der Updates verfügen.

3. Konfigurieren Sie Kaspersky Endpoint Security auf autonomen Geräten so, dass Updates aus einem lokalen Ordner oder von einer freigegebenen Ressource (FTP-Server oder freigegebener Ordner) heruntergeladen werden.

Anleitung:

- Hilfe zu Kaspersky Endpoint Security für Linux
- Hilfe zu Kaspersky Endpoint Security für Windows

4. Kopieren Sie die Update-Dateien von dem Wechseldatenträger in den lokalen Ordner oder auf die gemeinsam genutzte Ressource, die Sie als Update-Quelle nutzen wollen.

5. Starten Sie auf dem Offline-Gerät, das eine Update-Installation erfordert, die *Update*-Aufgabe von Kaspersky Endpoint Security für Linux oder Kaspersky Endpoint Security für Windows, je nach Betriebssystem des Offline-Geräts.

Nachdem die Update-Aufgabe abgeschlossen wurde, sind die Kaspersky-Datenbanken und Programm-Module auf diesem Gerät auf dem neuesten Stand.

Überwachung, Berichterstattung und Audit

In diesem Abschnitt werden die Möglichkeiten für die Überwachung und die Berichterstellung von Kaspersky Security Center Linux beschrieben. Diese Möglichkeiten geben Ihnen einen Überblick über Ihre Infrastruktur, die Schutzstatus und Statistiken.

Nach der Bereitstellung von Kaspersky Security Center Linux oder während des Programmbetriebs können Sie die Funktionen für die Überwachung und für die Berichterstellung an Ihre Bedürfnisse anpassen.

Szenario: Überwachung und Berichterstattung

Dieser Abschnitt enthält ein Szenario zur Konfiguration der Funktion der Überwachung und Berichterstellung in Kaspersky Security Center Linux.

Erforderliche Vorrausetzungen

Nach der Verteilung von Kaspersky Security Center Linux im Unternehmensnetzwerk können Sie mit seiner Überwachung beginnen und Berichte zum Netzwerkbetrieb erstellen.

Die Überwachung und Berichterstellung in einem Unternehmensnetzwerk erfolgt in mehreren Schritten:

1. **Wechsel der Statuswerte von Geräten konfigurieren**

   Machen Sie sich mit den Einstellungen des von bestimmten Bedingungen abhängigen Gerätestatus vertraut. Wenn Sie diese Einstellungen anpassen, können Sie auch die Anzahl der Ereignisse der Ereigniskategorie *Kritisch* oder *Warnung* ändern. Beachten Sie bei der Konfiguration des Wechsels des Gerätestatus Folgendes:

   - Die neuen Einstellungen widersprechen nicht den Richtlinien zur Informationssicherheit Ihres Unternehmens.
   - Sie können rechtzeitig auf wichtige Ereignisse der Informationssicherheit in Ihrem Unternehmensnetzwerk reagieren.

2. **Einstellungen für Benachrichtigungen über Ereignisse auf Client-Geräten anpassen**

   Anleitung:

   Passen Sie die Benachrichtigungen (per E-Mail, SMS oder durch Start einer ausführbaren Datei) zu Ereignissen auf Client-Geräten an

3. **Empfohlene Aktionen für kritische und warnende Benachrichtigungen ausführen**

   Anleitung:

   Führen Sie die empfohlenen Aktionen für Ihr Unternehmensnetzwerk aus

4. **Sicherheitsstatus Ihres Unternehmensnetzwerks verfolgen**

   Anleitung:

   - Sehen Sie sich das Widget Schutzstatus an
   - Erstellen und überprüfen Sie den Bericht über den Schutzstatus
   - Erstellen und überprüfen Sie den Fehlerbericht

5. **Client-Geräte finden, die nicht geschützt sind**

   Anleitung:

   - Sehen Sie sich das Widget Neue Geräte an
   - Erstellen und überprüfen Sie den Bericht über die Bereitstellung des Schutzes

6. **Schutz der Client-Geräte überprüfen**

   Anleitung:

   - Erstellen und lesen Sie Berichte der Kategorien Schutzstatus und Bedrohungsstatistiken
   - Starten und überprüfen Sie die Ereignisauswahl mit dem Wert "Kritisch"

7. **Ereignismenge für Datenbank einschätzen und einschränken**

   Informationen über Ereignisse im Betrieb der verwalteten Anwendungen werden vom Client-Gerät übertragen und in der Administrationsserver-Datenbank registriert. Um die Belastung auf den Administrationsserver zu reduzieren, sollten Sie die maximale Anzahl der Ereignisse, die in der Datenbank gespeichert werden können, einschätzen und einschränken.

   Anleitung:

   - Maximale Anzahl der Ereignisse einschränken

8. **Lizenzinformationen überprüfen**

   Anleitung:

   - Fügen Sie das Widget Nutzung von Lizenzschlüsseln zum Dashboard hinzu und sehen Sie es sich an
   - Erstellen und überprüfen Sie den Bericht über die Lizenzschlüsselnutzung

Ergebnisse

Nach Abschluss des Szenarios werden Sie über den Schutz Ihres Unternehmensnetzwerks informiert und können Aktionen für den weiteren Schutz des Netzwerks planen.

Über die Arten der Überwachung und Berichterstattung

Die Informationen über die Sicherheitsereignisse im Unternehmensnetzwerk werden in der Datenbank des Administrationsservers gespeichert. Basierend auf den Ereignissen bietet die Kaspersky Security Center Web Console die folgenden Arten der Überwachung und Berichterstattung in Ihrem Unternehmensnetzwerk:

- Dashboard
- Berichte
- Ereignisauswahlen
- Benachrichtigungen

Dashboard

Das Dashboard bietet eine grafische Darstellung von Informationen und erlaubt Ihnen, sicherheitsrelevante Entwicklungen in Ihrem Unternehmensnetzwerk zu überwachen.

Berichte

Mithilfe von Berichten können Sie detaillierte, zahlenbasierte Informationen zur Sicherheit Ihres Unternehmensnetzwerkes zusammenstellen und diese Informationen in einer Datei speichern, per E-Mail versenden und ausdrucken.

Ereignisauswahlen

Die Ereignisauswahlen bieten eine Bildschirmansicht der benannten Ereignisgruppen, die aus der Administrationsserver-Datenbank ausgewählt wurden. Diese Sätze von Ereignissen sind nach den folgenden Kategorien gruppiert:

- Nach Ereigniskategorie – **Kritische Ereignisse**, **Funktionsfehler**, **Warnungen** und **Informative Ereignisse**
- Nach Zeit – **Letzte Ereignisse**
- Nach Typ – **Benutzeranfragen** und **Audit-Ereignisse**

Benutzerdefinierte Ereignisauswahlen können Sie auf der Basis von Einstellungen, die in der Oberfläche von Kaspersky Security Center Web Console verfügbar sind, erstellen und anzeigen.

Benachrichtigungen

Benachrichtigungen informieren Sie über Ereignisse und unterstützen Sie dabei, mithilfe empfohlener Maßnahmen oder mit Maßnahmen, die Sie als geeignet erachten, schneller auf diese Ereignisse zu reagieren.

Auslösen von Regeln im Smart Training-Modus

Dieser Abschnitt enthält Informationen über die Funde, die mithilfe von Regeln der Adaptiven Kontrolle von Anomalien in Kaspersky Endpoint Security für Windows auf Client-Geräten erfolgt sind.

Die Regeln erkennen ungewöhnliches Verhalten auf Client-Geräten und können es blockieren. Wenn die Regeln im Smart Training-Modus ausgeführt werden, erkennen sie ungewöhnliches Verhalten und senden Berichte über jeden Fund an den Administrationsserver. Sie können die Berichte über erkanntes ungewöhnliches Verhalten unter **Datenverwaltung → Auslöser der Regel im Smart-Training-Status** anzeigen. Sie können Funde als korrekt bestätigen oder sie den Ausnahmen hinzufügen, damit solches Verhalten in Zukunft nicht mehr als ungewöhnlich registriert wird.

Informationen über Funde werden im Ereignisprotokoll auf dem Administrationsserver (gemeinsam mit anderen Ereignissen) und im Bericht über die Adaptive Kontrolle von Anomalien gespeichert.

Weitere Informationen über die Regeln für die Adaptive Kontrolle von Anomalien, deren Modi und Status finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

Anzeigen und Bestätigen von Funden, die auf Regeln der Adaptiven Kontrolle von Anomalien beruhen

So zeigen Sie die Liste der Funde mithilfe der Regeln für die Adaptive Kontrolle von Anomalien an:

1. Wechseln Sie im Hauptmenü zu **Datenverwaltung → Auslöser der Regel im Smart-Training-Status**.

   Die Liste enthält die folgenden Informationen zu den Funden mithilfe der Regeln für die Adaptive Kontrolle von Anomalien:

   - **Administrationsgruppe**

     Name der Administrationsgruppe, zu der das Gerät gehört.

   - **Virtueller Administrationsserver**

     Virtueller Administrationsserver, der das Gerät verwaltet.

   - **Gerätename**

     Name des Client-Geräts, auf das die Regel angewendet wurde.

   - **Name**

     Name der Regel, die angewendet wurde.

   - **Status**

     Excluding – Wenn der Administrator dieses Element verarbeitet und als Ausnahme für die Regeln hinzugefügt hat. Dieser Status bleibt bis zur nächsten Synchronisierung des Client-Geräts mit dem Administrationsserver bestehen; nach der Synchronisierung wird das Element aus der Liste entfernt.

     Confirming – Wenn der Administrator dieses Element verarbeitet und bestätigt hat. Dieser Status bleibt bis zur nächsten Synchronisierung des Client-Geräts mit dem Administrationsserver bestehen; nach der Synchronisierung wird das Element aus der Liste entfernt.

     Leer – Wenn der Administrator dieses Element nicht verarbeitet hat.

   - **Anzahl der Funde**

     Anzahl der Funde für eine heuristische Regel, einen Prozess und ein Client-Gerät. Diese Anzahl wird von Kaspersky Endpoint Security berechnet.

   - **Benutzername**

     Name des Benutzers des Client-Geräts, der den Prozess ausgeführt hat, welcher den Fund erzeugt hat.

   - **Pfad des Quellprozesses**

     Pfad des Quellprozesses, d. h. des Prozesses, der die Aktion durchführt (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

   - **Hash des Quellprozesses**

     SHA256-Hash der Datei des Quellprozesses (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Pfad des Quellobjekts**

  Pfad des Objekts, das den Prozess, gestartet hat (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Hash des Quellobjekts**

  SHA256-Hash der Quelldatei (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Pfad des Zielprozesses**

  Pfad des Zielprozesses (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Hash des Zielprozesses**

  SHA256-Hash der Zieldatei (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Pfad des Zielobjekts**

  Pfad des Zielobjekts (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Hash des Zielobjekts**

  SHA256-Hash der Zieldatei (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security).

- **Bearbeitet**

  Datum, an dem die Anomalie gefunden wurde.

So zeigen Sie die Eigenschaften eines Fundes an:

1. Wechseln Sie im Hauptmenü zu **Datenverwaltung** → **Auslöser der Regel im Smart-Training-Status**.
2. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie in der Spalte **Name** auf den Link mit dem Namen des Fundes, den Sie anzeigen möchten.
   - Aktivieren Sie in der Liste der Funde das Kontrollkästchen neben dem Fund, den Sie anzeigen möchten, und klicken Sie anschließend auf **Eigenschaften**.

   Für den ausgewählten Fund öffnet sich das Eigenschaftsfenster mit Informationen zu dem Fund.

Sie können jeden Fund entweder aus der Liste mit den Funden, die von den Regeln der Adaptiven Kontrolle von Anomalien erkannt wurden, oder direkt aus dem Eigenschaftsfenster eines ausgewählten Fundes bestätigen.

So bestätigen Sie einen Fund:

- Wählen Sie in der Liste mit den Funden mindestens einen Fund aus und klicken Sie anschließend auf die Schaltfläche **Bestätigen**.
- Öffnen Sie das Eigenschaftsfenster eines ausgewählten Fundes und klicken Sie anschließend auf die Schaltfläche **Bestätigen**.

Der Status der gewählten Elemente ändert sich zu **Bestätigung**. Der Fund wird nach der nächsten Synchronisierung des Client-Geräts mit dem Administrationsserver aus der Liste der Funde entfernt.

Ihre Bestätigung trägt zu den Statistiken bei, die von den Regeln verwendet werden. Weitere Informationen dazu finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

Ausschlüsse aus den Regeln zur Adaptiven Kontrolle von Anomalien hinzufügen

Mit dem Assistenten zum Hinzufügen von Ausnahmen zur Adaptiven Kontrolle von Anomalien können Sie Ausnahmen für Regeln der Adaptiven Kontrolle von Anomalien in Kaspersky Endpoint Security hinzufügen.

So fügen Sie mithilfe des Assistenten Ausnahmen zu den Regeln der Adaptiven Kontrolle von Anomalien hinzu:

1. Starten Sie den Assistenten auf eine der folgenden Arten:

   - Wechseln Sie im Hauptmenü zu **Datenverwaltung** → **Auslöser der Regel im Smart-Training-Status**, wählen Sie mindestens einen Fund und klicken Sie anschließend die auf Schaltfläche **Ausschließen**.

     Sie können bis zu 1000 Ausschlüsse auf einmal hinzufügen.

     Bevor Sie einen Fund zu den Ausschlüssen hinzufügen, können Sie die Eigenschaften des Fundes anzeigen, indem Sie auf den Namen des Fundes oder auf die Schaltfläche **Eigenschaften** klicken. Im neuen Eigenschaftsfenster des Fundes können Sie ebenfalls die auf Schaltfläche **Ausschließen** klicken.

   - Wechseln Sie im Hauptmenü zu **Überwachung** → **Ereignisauswahlen**, klicken Sie auf den Link der erforderlichen Auswahl, aktivieren Sie das Kontrollkästchen neben dem Fund, den Sie ausschließen möchten, und klicken Sie anschließend auf die Schaltfläche **Aus Adaptiver Kontrolle von Anomalien ausschließen**.

   Der Assistent zum Hinzufügen einer Ausnahme zur Adaptive Kontrolle von Anomalien wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

2. Wählen Sie alle Richtlinien und Profile aus, denen Sie Ausnahmen hinzufügen möchten.

   Geerbte Richtlinien können nicht aktualisiert werden. Wenn Sie keine Berechtigungen zum Ändern einer Richtlinie haben, wird die Richtlinie nicht aktualisiert.

3. Klicken Sie auf **Fertig**, um den Assistenten zu schließen.

Der Status der gewählten Elemente ändert sich zu **Ausschluss wird erstellt**. Der Fund wird nach der nächsten Synchronisierung des Client-Geräts mit dem Administrationsserver aus der Liste der Funde entfernt. Die Ausnahme für Regeln der Adaptiven Kontrolle von Anomalien ist jetzt konfiguriert und wird angewendet.

Dashboard und Widgets

Dieser Abschnitt enthält Informationen über das Dashboard und die Widgets, die vom Dashboard bereitgestellt werden. Der Abschnitt enthält Anweisungen zum Verwalten von Widgets und zum Konfigurieren von Widget-Einstellungen.

Dashboard verwenden

Das Dashboard bietet eine grafische Darstellung von Informationen und erlaubt Ihnen, sicherheitsrelevante Entwicklungen in Ihrem Unternehmensnetzwerk zu überwachen.

Das Dashboard finden Sie in der Kaspersky Security Center Web Console im Abschnitt **Überwachung** unter **Dashboard**.

Das Dashboard enthält Widgets, die angepasst werden können. Sie können aus einer großen Anzahl an unterschiedlichen Widgets auswählen, die als Kreis- oder Ringdiagramme, Tabellen, Grafiken, Balkendiagramme und Listen dargestellt werden. Die in den Widgets angezeigten Informationen werden automatisch aktualisiert und das Aktualisierungsintervall beträgt ein bis zwei Minuten. Das Aktualisierungsintervall unterscheidet sich von Widget zu Widget. Über das Einstellungsmenü können Sie die Daten eines Widgets jederzeit manuell aktualisieren.

Standardmäßig enthalten Widgets Informationen über alle Ereignisse, die in der Datenbank des Administrationsservers gespeichert sind.

Die Kaspersky Security Center Web Console besitzt eine Standardauswahl an Widgets der folgenden Kategorien:

- **Schutzstatus**
- **Bereitstellung**
- **Aktualisierungen**
- **Bedrohungsstatistiken**
- **Andere**

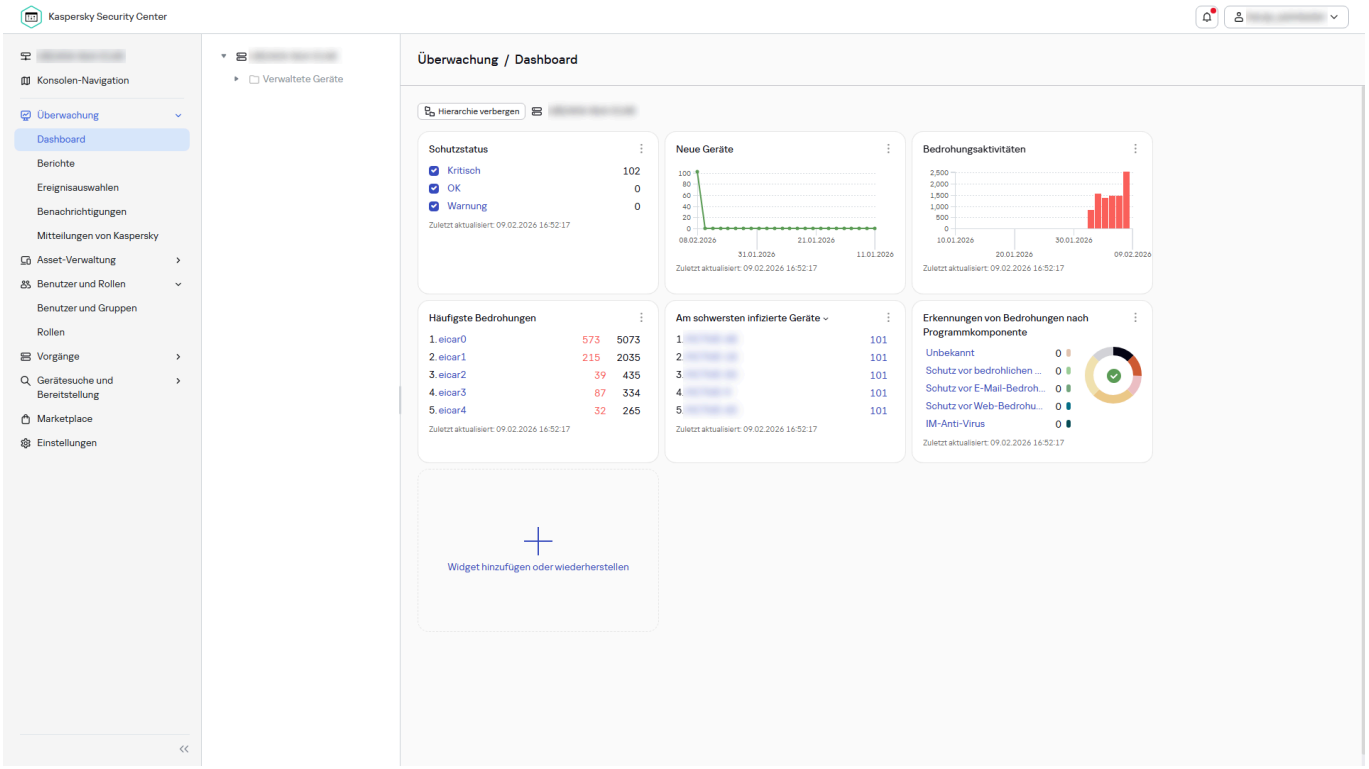
Einige Widgets enthalten Textinformationen und Links. Über einen Link können ausführliche Informationen angezeigt werden.

Bei der Konfiguration des Dashboards können Sie gewünschte Widgets hinzufügen, nicht benötigte Widgets ausblenden, die Größe und Darstellung der Widgets ändern, Widgets verschieben und ihre Einstellungen anpassen.

Dem Dashboard Widgets hinzufügen

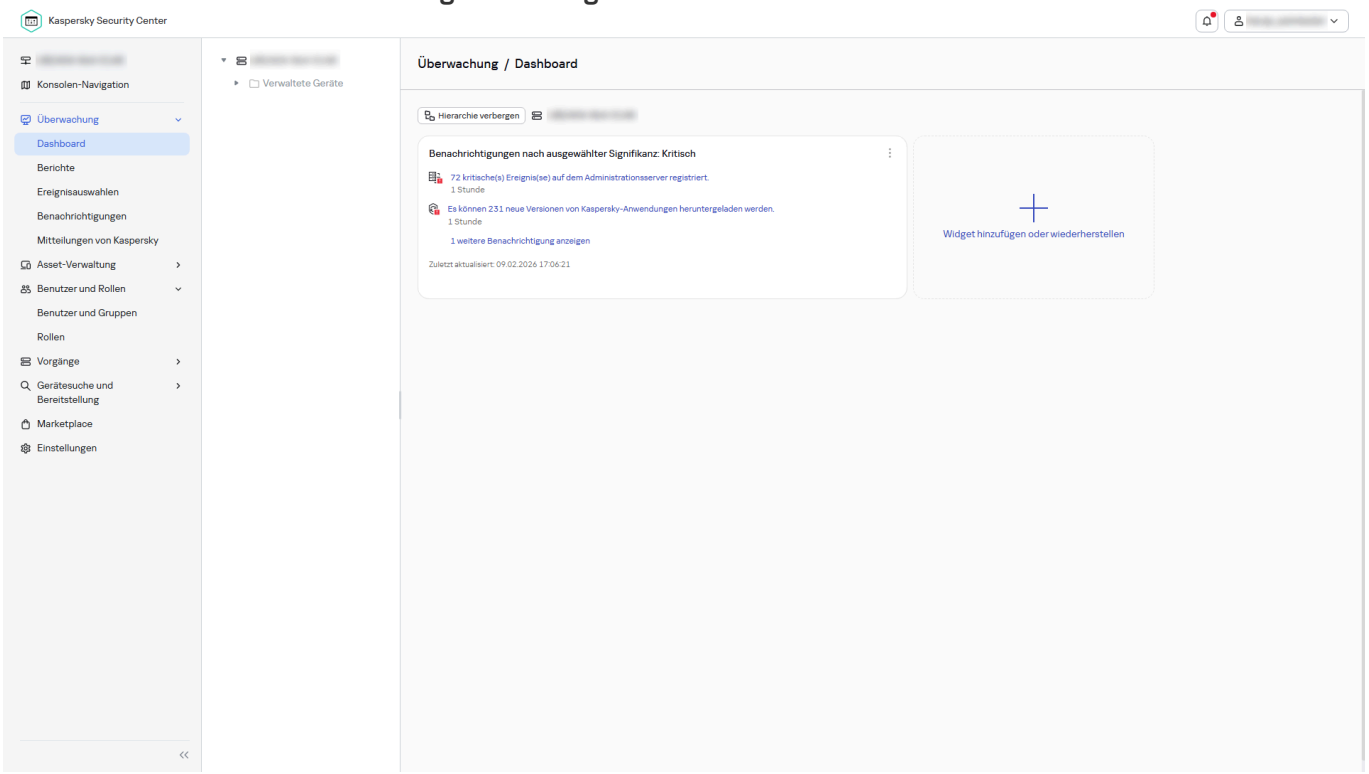
So fügen Sie Widgets zum Dashboard hinzu:

1. Wechseln Sie im Hauptmenü zu **Überwachung → Dashboard**.



Das Dashboard mit Widgets

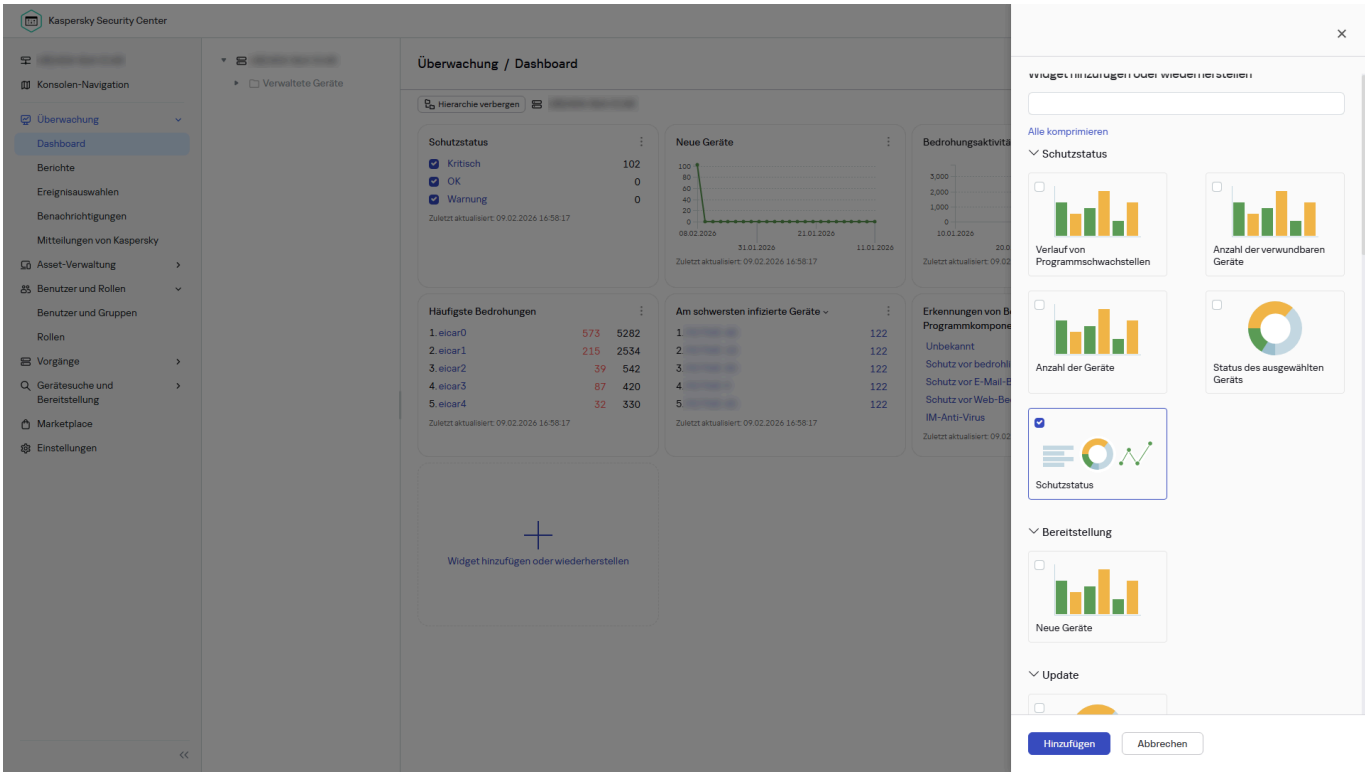
2. Klicken Sie auf die Schaltfläche **Widget hinzufügen oder wiederherstellen**.



Hinzufügen eines Widgets

3. Wählen Sie in der Liste der verfügbaren Widgets die Widgets aus, die Sie dem Dashboard hinzufügen möchten.

   Widgets sind nach Kategorien gruppiert. Um die Liste der in einer Kategorie enthaltenen Widgets anzuzeigen, klicken Sie auf das Chevron-Symbol (>) neben dem Kategorienamen.



Auswählen des Widget-Typs

4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

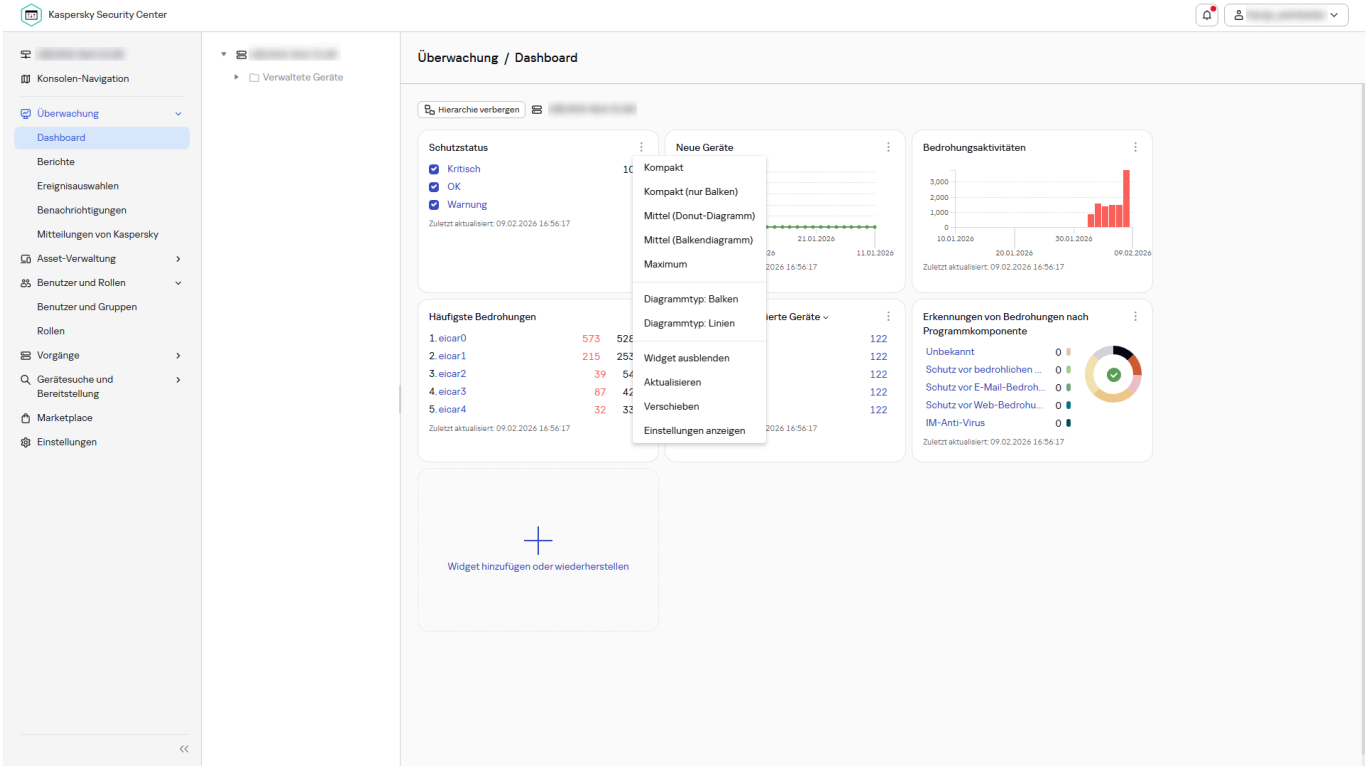
   Die ausgewählten Widgets werden am Ende des Dashboards hinzugefügt.

   Sie können jetzt die Darstellung und Parameter der hinzugefügten Widgets bearbeiten.

Widgets im Dashboard verbergen

So verbergen Sie ein angezeigtes Widget im Dashboard:

1. Gehen Sie im Hauptmenü zu **Überwachung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie ausblenden möchten.



Das Widget-Menü

3. Wählen Sie **Widget ausblenden** aus.
4. Klicken Sie im folgenden Fenster **Warnung** auf **OK**.

Das ausgewählte Widget wird verborgen. Später können Sie dieses Widget erneut zum Dashboard hinzufügen.

Widgets auf dem Dashboard verschieben

So verschieben Sie ein Widget im Dashboard:

1. Gehen Sie im Hauptmenü zu **Überwachung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie verschieben möchten.
3. Wählen Sie **Verschieben** aus.
4. Klicken Sie auf die Position, an die Sie das Widget verschieben möchten. Sie können nur ein anderes Widget auswählen.

Die Positionen der ausgewählten Widgets werden vertauscht.

Größe oder Darstellung von Widgets ändern

Bei Widgets, die ein Diagramm anzeigen, können Sie dessen Darstellung ändern - ein Balkendiagramm oder Liniendiagramms. Bei einigen Widgets können Sie ihre Größe ändern: kompakt, mittel oder maximal.

So ändern Sie die Widget-Darstellung:

1. Wechseln Sie im Hauptmenü zu **Überwachung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie bearbeiten möchten.
3. Führen Sie eine der folgenden Aktionen aus:
   - Um ein Widget als Balkendiagramm anzuzeigen, wählen Sie **Diagrammtyp: Balken** aus.
   - Um ein Widget als Liniendiagramm anzuzeigen, wählen Sie **Diagrammtyp: Linien** aus.
   - Um die vom Widget eingenommene Fläche zu ändern, wählen Sie einen der Werte:
     - **Kompakt**
     - **Kompakt (nur Balken)**
     - **Mittel (Donut-Diagramm)**
     - **Mittel (Balkendiagramm)**
     - **Maximum**

Die Darstellung des ausgewählten Widgets wird geändert.

Einstellungen von Widgets ändern

Um die Einstellungen eines Widgets zu ändern, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie ändern möchten.
3. Wählen Sie **Einstellungen anzeigen** aus.
4. Ändern Sie im folgenden Fenster mit den Widgeteinstellungen die Widgeteinstellungen nach Bedarf.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die Einstellungen des ausgewählten Widgets werden geändert.

Der Satz an Einstellungen hängt vom jeweiligen Widget ab. Nachfolgend finden Sie einige allgemeine Einstellungen:

- **Anwendungsbereich des Widgets** (Auswahl an Objekten, für die das Widget Informationen anzeigt) – Zum Beispiel eine Administrationsgruppe oder eine Geräteauswahl.
- **Aufgabe auswählen** (Aufgabe, für die das Widget Informationen anzeigt).
- **Zeitintervall** (Zeitintervall, während dem die Informationen im Widget angezeigt werden) – Zwischen zwei angegebenen Zeitpunkten; vom angegebenen Zeitpunkt bis zum aktuellen Tag; oder vom aktuellen Tag abzüglich der angegebenen Anzahl von Tagen bis zum aktuellen Tag.
- **Bekommt den Status "Kritisch" zugewiesen, wenn folgende Bedingungen erfüllt sind** und **Bekommt den Status "Warnung" zugewiesen, wenn folgende Bedingungen erfüllt sind** (Regeln, welche die Farbe eines farblichen Indikators festlegen).

Nachdem Sie die Widget-Einstellungen geändert haben, können Sie die Daten im Widget manuell aktualisieren.

So aktualisieren Sie Daten in einem Widget:

1. Wechseln Sie im Hauptmenü zu **Überwachung** → **Dashboard**.
2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie verschieben möchten.
3. Wählen Sie **Aktualisieren** aus.

Die Daten im Widget werden aktualisiert.

Über den Nur-Dashboard-Modus

Für Mitarbeiter, die das Netzwerk nicht verwalten, aber die Statistiken zum Netzwerkschutz in Kaspersky Security Center Linux anzeigen möchten (z. B. ein Top-Manager) können Sie den Nur-Dashboard-Modus konfigurieren. Wenn dieser Modus bei einem Benutzer aktiviert ist, wird dem Benutzer nur ein Dashboard mit einem vordefinierten Satz von Widgets angezeigt. So kann er oder sie die in den Widgets angegebenen Statistiken, wie den Schutzstatus aller verwalteten Geräte, die Anzahl der zuletzt erkannten Bedrohungen oder die Liste der häufigsten Bedrohungen im Netzwerk, überwachen.

Wenn ein Benutzer im Nur-Dashboard-Modus arbeitet, gelten die folgenden Einschränkungen:

- Das Hauptmenü wird dem Benutzer nicht angezeigt, sodass er die Schutzeinstellungen für das Netzwerk nicht ändern kann.
- Der Benutzer kann mit Widgets keine Aktionen, wie hinzufügen oder ausblenden, ausführen. Daher müssen Sie alle für den Benutzer erforderlichen Widgets auf dem Dashboard platzieren und konfigurieren, indem Sie etwa die Regel zum Zählen von Objekten oder das Zeitintervall festlegen.

Sie können sich den Nur-Dashboard-Modus nicht selbst zuweisen. Wenn Sie in diesem Modus arbeiten möchten, wenden Sie sich an einen Systemadministrator, Managed Service Provider (MSP) oder einen Benutzer mit der Berechtigung **Objekt-ACLs ändern** im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen**.

Nur-Dashboard-Modus konfigurieren

Bevor Sie mit der Konfiguration des Nur-Dashboard-Modus beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Sie besitzen die Berechtigung **Objekt-ACLs ändern** in dem Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen**. Wenn Sie diese Berechtigung nicht besitzen, fehlt der Reiter zur Konfiguration des Modus.
- Der Benutzer besitzt die Berechtigungen **Lesen** in dem Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen**.

> Wenn in Ihrem Netzwerk eine Hierarchie von Administrationsservern eingerichtet ist, wechseln Sie zur Konfiguration des Nur-Dashboard-Modus auf den Server, auf dem das Benutzerkonto auf der Registerkarte **Benutzer** des Abschnitts **Benutzer und Rollen → Benutzer und Gruppen** verfügbar ist. Dabei kann es sich um einen primären oder einen physischen sekundären Server handeln. Es ist nicht möglich, den Modus auf einem virtuellen Server zu konfigurieren.

So konfigurieren Sie den Nur-Dashboard-Modus:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen → Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Klicken Sie auf den Namen des Benutzerkontos, für welches Sie das Dashboard mit Widgets anpassen möchten.
3. Öffnen Sie im folgenden Fenster mit den Kontoeinstellungen die Registerkarte **Dashboard**.

   Auf der sich öffnenden Registerkarte wird Ihnen das gleiche Dashboard angezeigt wie dem Benutzer.
4. Wenn die Option **Konsole im Nur-Dashboard-Modus anzeigen** aktiviert ist, klicken Sie auf den Umschalter, um sie zu deaktivieren.

   Wenn diese Option aktiviert ist, können auch Sie das Dashboard nicht ändern. Nachdem Sie die Option deaktiviert haben, können Sie Widgets verwalten.
5. Konfigurieren Sie das Erscheinungsbild des Dashboards. Der auf der Registerkarte **Dashboard** angezeigte Satz von Widgets steht dem Benutzer mit dem anpassbaren Konto zur Verfügung. Er oder sie kann weder die Einstellungen noch die Größe der Widgets ändern, und keine Widgets zum Dashboard hinzufügen oder daraus entfernen. Daher müssen Sie für den Benutzer die Widgets anpassen, damit er oder sie die Statistiken zum Netzwerkschutz anzeigen kann. Um dies zu tun, können Sie auf der Registerkarte **Dashboard** die gleichen Vorgänge mit den Widgets ausführen, wie im Abschnitt **Überwachung → Dashboard**:
   - Dem Dashboard neue Widgets hinzufügen.
   - Vom Nutzer nicht benötigte Widgets ausblenden.
   - Widgets verschieben, sodass sie einer bestimmten Reihenfolge entsprechen.
   - Die Größe oder das Aussehen von Widgets ändern.
   - Die Einstellungen von Widgets ändern.
6. Klicken Sie auf den Umschalter, um die Option **Konsole im Nur-Dashboard-Modus anzeigen** zu aktivieren.

Anschließend steht dem Benutzer nur noch das Dashboard zur Verfügung. Er oder sie kann Statistiken überwachen, aber die Schutzeinstellungen des Netzwerks und das Erscheinungsbild des Dashboards nicht ändern. Da für Sie das gleiche Dashboard wie für den Benutzer angezeigt wird, können auch Sie das Dashboard nicht ändern.

Wenn Sie die Option deaktiviert lassen, wird dem Benutzer das Hauptmenü angezeigt, sodass er verschiedene Aktionen in Kaspersky Security Center Linux ausführen kann, einschließlich der Änderung von Sicherheitseinstellungen und Widgets.

7. Wenn Sie die Konfiguration des Nur-Dashboard-Modus abgeschlossen haben, klicken Sie auf **Speichern**. Erst im Anschluss wird dem Benutzer das konfigurierte Dashboard angezeigt.

8. Wenn der Benutzer zum Anzeigen der Statistiken von unterstützten Kaspersky-Anwendungen spezielle Zugriffsrechte benötigt, konfigurieren Sie diese Rechte für den Benutzer. Anschließend werden für den Benutzer die Daten der Kaspersky-Anwendungen in ihren entsprechenden Anwendungs-Widgets angezeigt.

Der Benutzer kann sich jetzt mit dem angepassten Benutzerkonto an Kaspersky Security Center Linux anmelden und die Statistiken zum Netzwerkschutz im Nur-Dashboard-Modus überwachen.

Verwaltungs- und Schutzberichte

In diesem Abschnitt wird beschrieben, wie Sie Berichte verwenden, benutzerdefinierte Berichtsvorlagen verwalten, Berichtsvorlagen zum Generieren neuer Berichte verwenden und Aufgaben zum Berichtsversand erstellen.

Berichte verwenden

Mithilfe von Berichten können Sie detaillierte, zahlenbasierte Informationen zur Sicherheit Ihres Unternehmensnetzwerkes zusammenstellen und diese Informationen in einer Datei speichern, per E-Mail versenden und ausdrucken.

Berichte finden Sie in der Kaspersky Security Center Web Console in dem Abschnitt **Überwachung** unter **Berichte**.

Standardmäßig enthalten Berichte Informationen für die letzten 30 Tage.

Kaspersky Security Center Linux besitzt eine Standardauswahl an Berichten für die folgenden Kategorien:

- **Schutzstatus**
- **Bereitstellung**
- **Aktualisierungen**
- **Bedrohungsstatistiken**
- **Andere**

Sie können eigene Berichtsvorlagen erstellen, Berichtsvorlagen bearbeiten und löschen.

Sie können Berichte erstellen, die auf vorhandenen Vorlagen basieren, Berichte in eine Datei exportieren und Aufgaben zum Versand von Berichten erstellen.

Berichtsvorlage erstellen

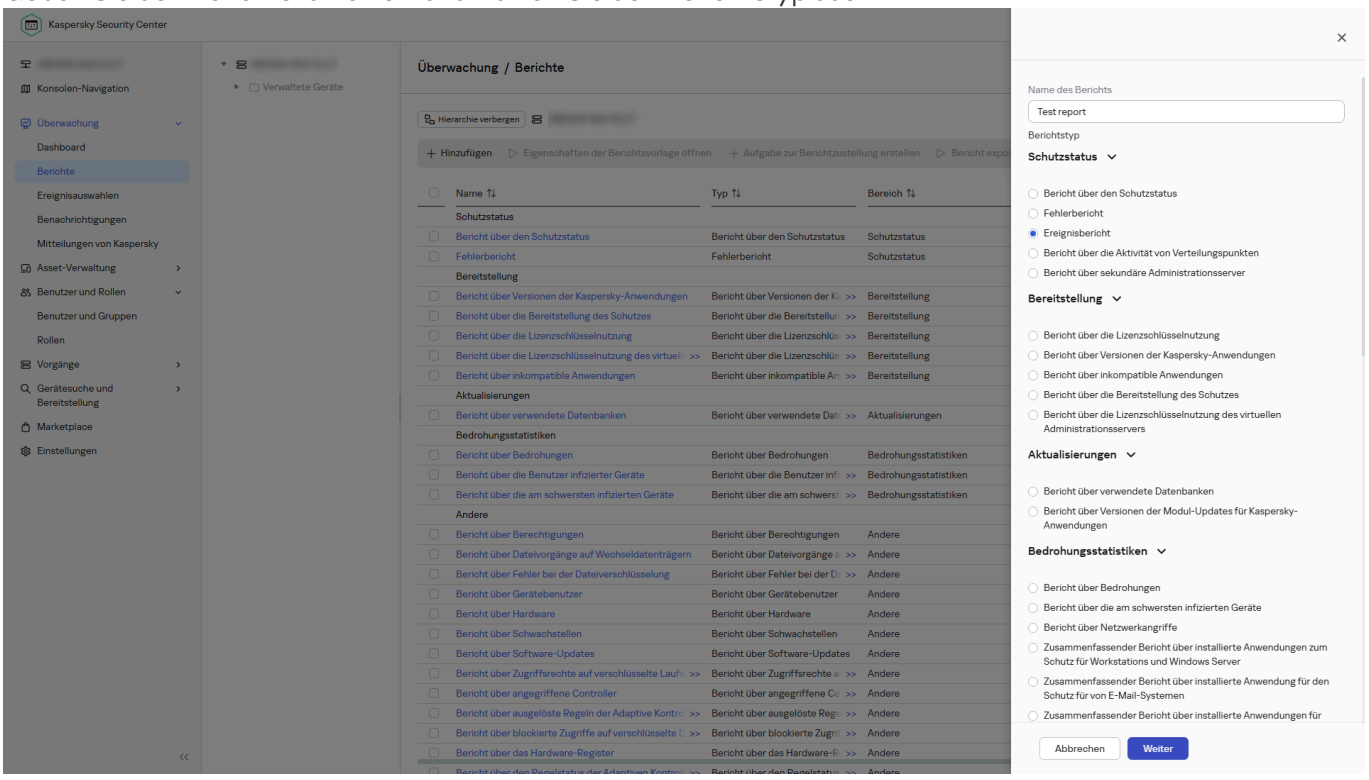
Um eine Berichtsvorlage zu erstellen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Überwachung** → **Berichte**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

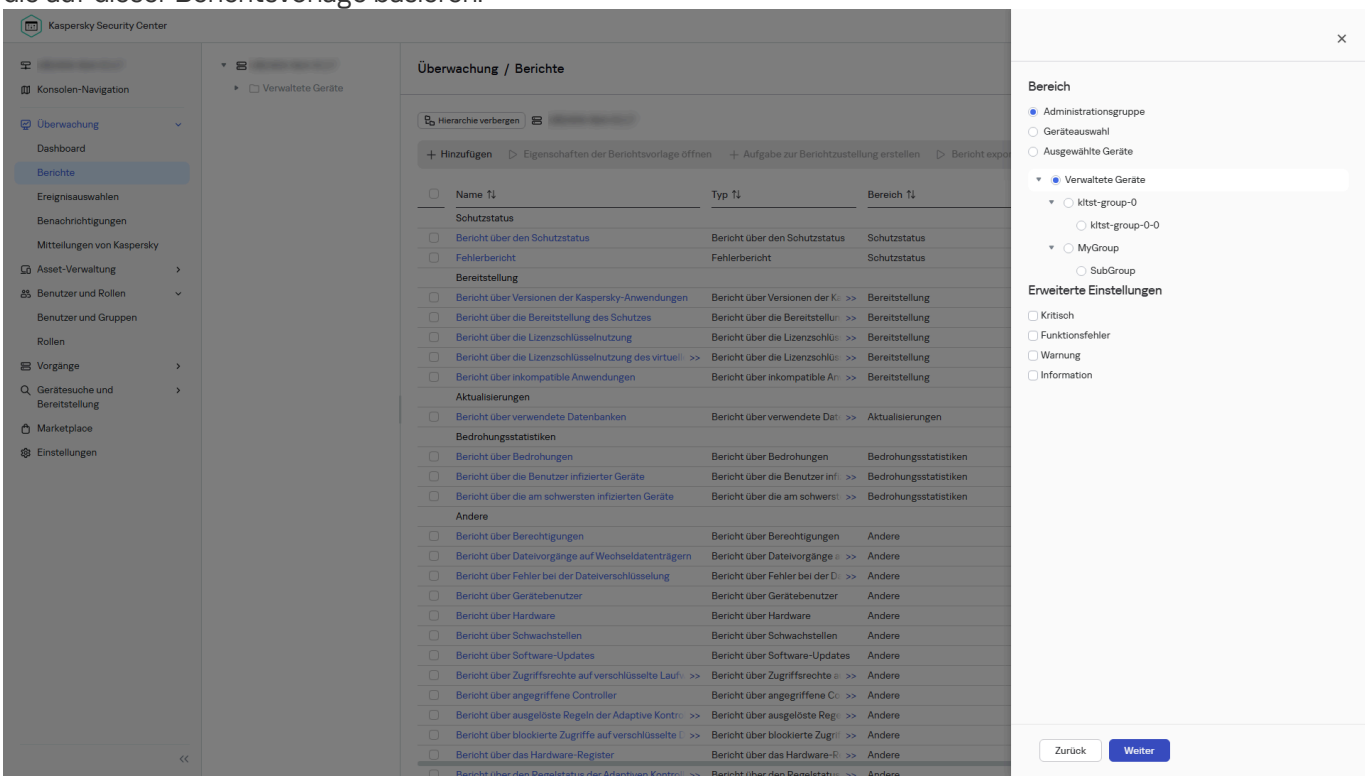
   Daraufhin wird der Assistent für das Erstellen einer Berichtsvorlage gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Geben Sie den Berichtsnamen ein und wählen Sie den Berichtstyp aus.



Angeben des Namens des Berichts und Auswählen des Berichtstyps

4. Wählen Sie im Schritt **Bereich** des Assistenten den Satz an Client-Geräten aus (Administrationsgruppe, Geräteauswahl, ausgewählte Geräte oder alle Geräte im Netzwerk), deren Daten in Berichten angezeigt werden, die auf dieser Berichtsvorlage basieren.

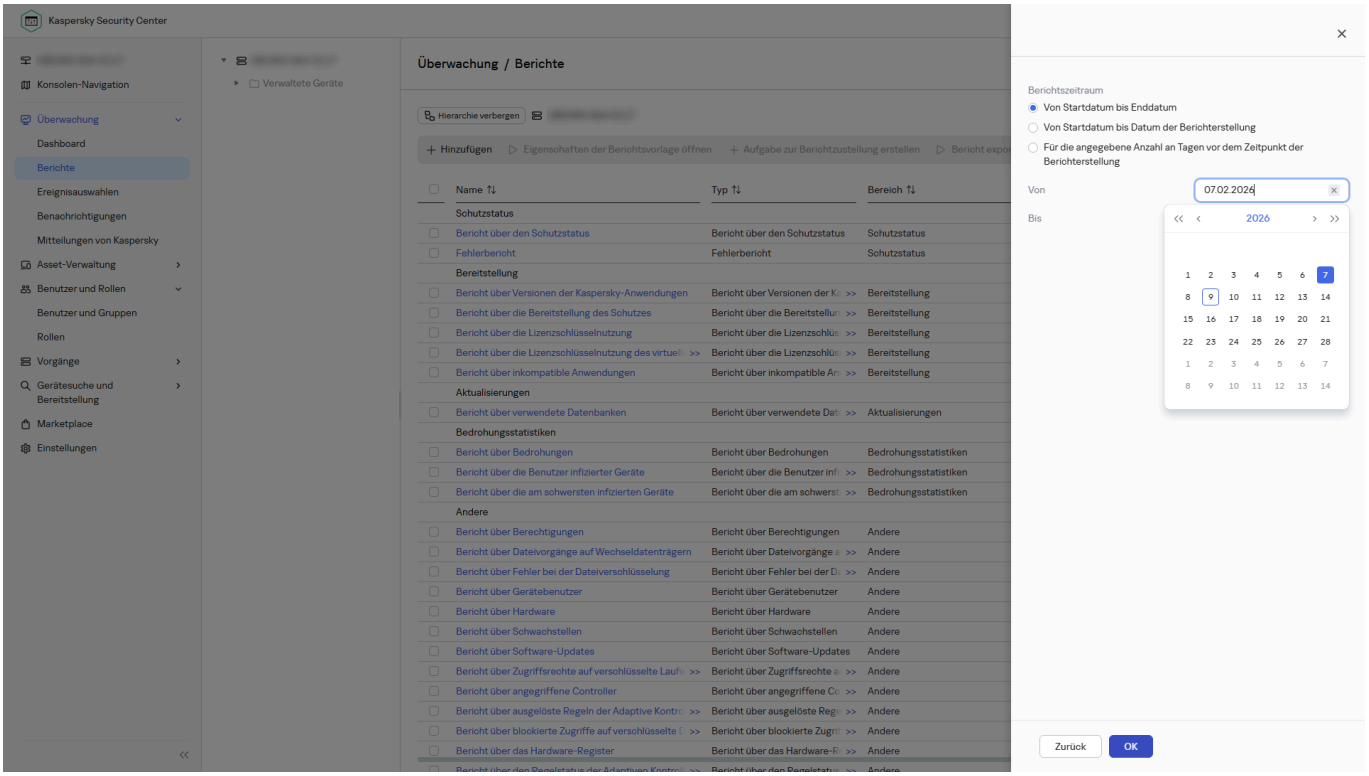


Angeben des Berichtsumfangs

5. Legen Sie im Schritt **Berichtszeitraum** des Assistenten den Berichtszeitraum fest. Die folgenden Werte sind verfügbar:

   - Zwischen den beiden angegebenen Daten
   - Vom angegebenen Datum bis zum Erstellungsdatum des Berichts
   - Vom angegebenen Datum der Berichterstellung abzüglich der Tage bis zum Erstellungsdatum des Berichts

Diese Seite wird nicht in allen Berichten angezeigt.



Angeben des Berichtszeitraums

6. Klicken Sie auf **OK**, um den Assistenten zu schließen.

7. Führen Sie eine der folgenden Aktionen aus:

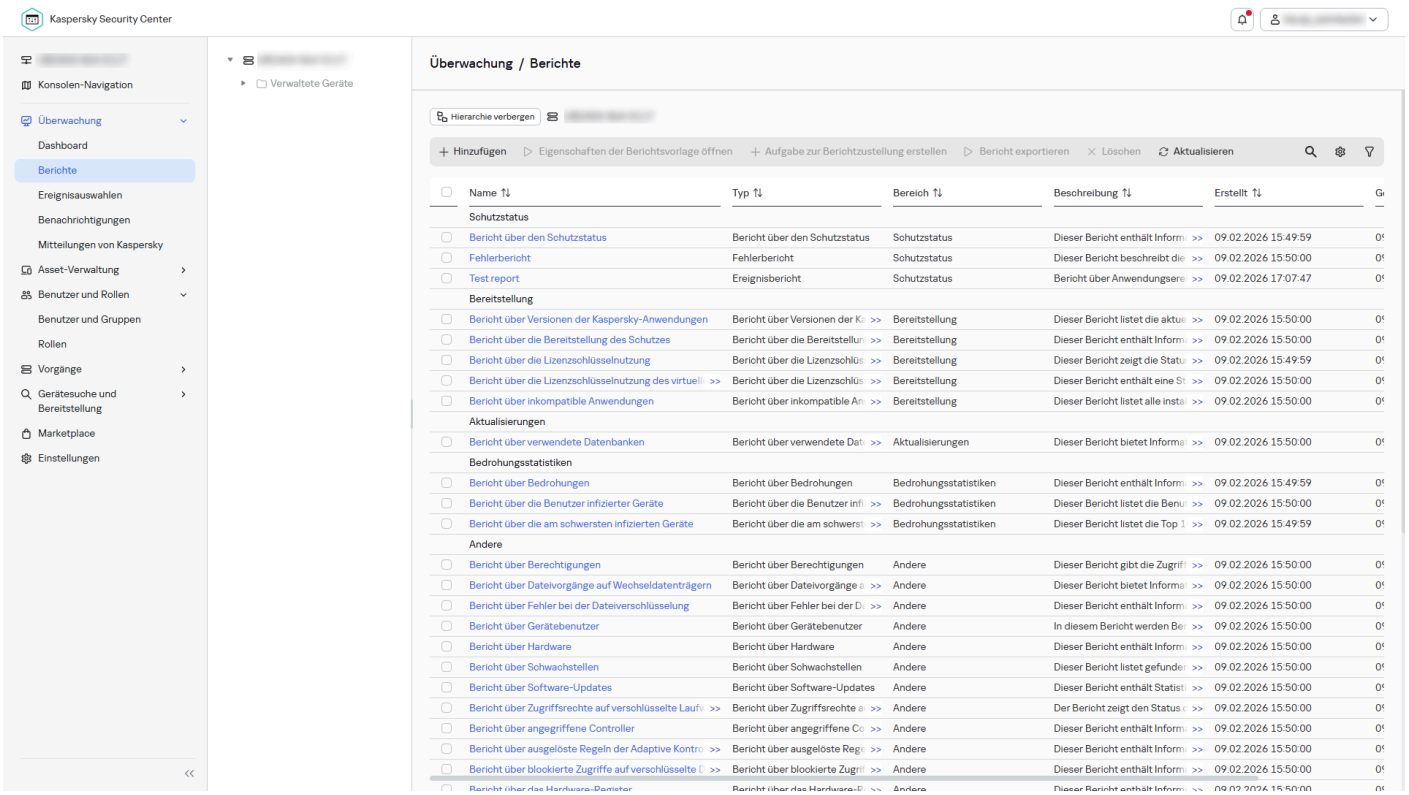
   - Klicken Sie auf die Schaltfläche **Speichern und ausführen**, um die neue Berichtsvorlage zu speichern und darauf basierend einen Bericht auszuführen.

     Die Berichtsvorlage wird gespeichert. Der Bericht wird generiert.

   - Klicken Sie auf die Schaltfläche **Speichern**, um die neue Berichtsvorlage zu speichern.

     Die Berichtsvorlage wird gespeichert.

Diese neue Vorlage kann nun zum Erstellen und Anzeigen von Berichten verwendet werden.



Die Liste der Berichte

Eigenschaften von Berichtsvorlagen anzeigen und bearbeiten

Sie können grundlegenden Eigenschaften einer Berichtsvorlage anzeigen und ändern, beispielsweise den Namen der Berichtsvorlage oder die im Bericht angezeigten Felder.

Um die Eigenschaften einer Berichtsvorlage anzuzeigen und zu ändern, gehen Sie wie folgt vor:

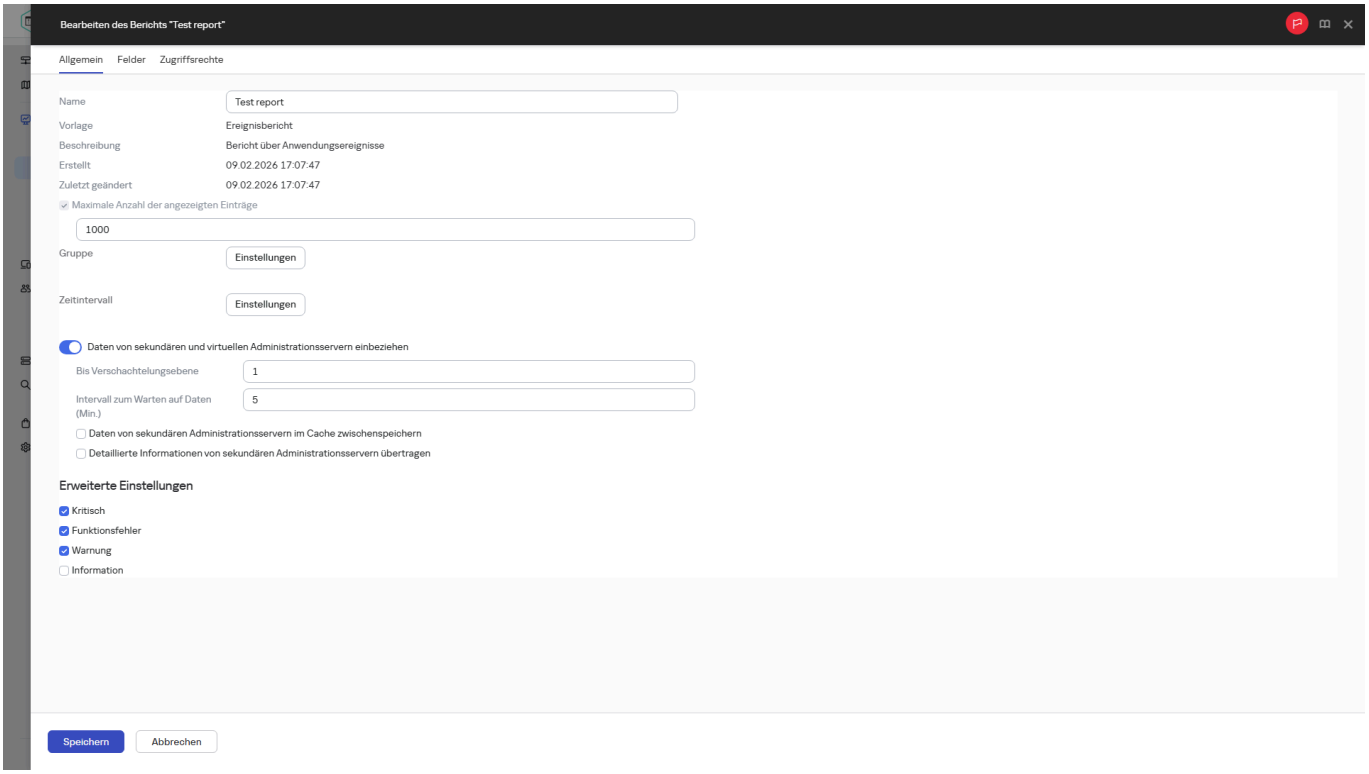
1. Wechseln Sie im Hauptmenü zu **Überwachung** → **Berichte**.

2. Aktivieren Sie das Kontrollkästchen neben der Berichtsvorlage, deren Eigenschaften Sie anzeigen und ändern möchten.

   Alternativ dazu können Sie zuerst den Bericht generieren und dann auf die Schaltfläche **Bearbeiten** klicken.

3. Klicken Sie auf die Schaltfläche **Eigenschaften der Berichtsvorlage öffnen**.

Das Fenster **Bearbeiten des Berichts <Berichtsname>** wird geöffnet, in dem die Registerkarte **Allgemein** ausgewählt ist.



Die Eigenschaften der Berichtsvorlage

4. Bearbeiten Sie die Eigenschaften der Berichtsvorlagen:

- Registerkarte **Allgemein**:
  - Name der Berichtsvorlage
  - **Maximale Anzahl der angezeigten Einträge**

    Wenn diese Option aktiviert ist, übersteigt die Anzahl der Einträge in der Tabelle mit detaillierten Berichtsdaten den angegebene Wert nicht. Beachten Sie, dass beim Exportieren des Berichts in eine Datei diese Option keinen Einfluss auf die maximale Anzahl von aufzunehmenden Ereignissen hat.

    Die Berichtseinträge werden zuerst nach den Regeln sortiert, die im Abschnitt **Felder** → **Detail-Felder** der Eigenschaften der Berichtsvorlage angegeben sind, und nur der erste der resultierenden Einträge wird beibehalten. Die Überschrift der Tabelle mit detaillierten Berichtsdaten zeigt die angezeigte Anzahl von Einträgen und die insgesamt verfügbare Anzahl von Einträgen, die mit anderen Berichtsvorlageneinstellungen übereinstimmen.

    Wenn diese Option deaktiviert ist, zeigt die Tabelle mit detaillierten Berichtsdaten alle verfügbaren Einträge an. Es wird nicht empfohlen, diese Option zu deaktivieren. Durch die Begrenzung der Anzahl der angezeigten Berichtseinträge wird das Datenbankverwaltungssystem (DBMS) entlastet und der Zeitaufwand für das Generieren und Exportieren des Berichts verringert. Einige der Berichte enthalten zu viele Einträge. Wenn dies der Fall ist, kann es schwierig sein, sie alle zu lesen und zu analysieren. Außerdem kann es sein, dass die Erstellung eines solchen Berichts zu einer Erschöpfung der Speicherressourcen Ihres Geräts führt und Sie den Bericht dann nicht ansehen können.

    Diese Option ist standardmäßig aktiviert. Als Standardwert ist 1000 vorgegeben.

  - **Gruppe**

    Klicken Sie auf die Schaltfläche **Einstellungen**, um den Satz an Client-Geräten zu ändern, für die der Bericht erstellt wird. Bei einigen Arten von Berichten ist die Schaltfläche möglicherweise nicht verfügbar. Die aktuellen Einstellungen hängen von den Einstellungen ab, die bei der Erstellung der Berichtsvorlage angegeben wurden.

- **Zeitintervall**

  Klicken Sie auf die Schaltfläche **Einstellungen**, um den Berichtszeitraum zu ändern. Bei einigen Arten von Berichten ist die Schaltfläche möglicherweise nicht verfügbar. Die folgenden Werte sind verfügbar:

  - Zwischen den beiden angegebenen Daten
  - Vom angegebenen Datum bis zum Erstellungsdatum des Berichts
  - Vom angegebenen Datum der Berichterstellung abzüglich der Tage bis zum Erstellungsdatum des Berichts

- **Daten von sekundären und virtuellen Administrationsservern einbeziehen**

  Wenn diese Option aktiviert ist, umfasst der Bericht die Informationen vom sekundären und vom virtuellen Administrationsserver, die dem Administrationsserver untergeordnet sind, für den die Berichtsvorlage erstellt wurde.

  Deaktivieren Sie diese Option, wenn Sie nur Daten vom aktuellen Administrationsserver anzeigen möchten.

  Diese Option ist standardmäßig aktiviert.

- **Bis Verschachtelungsebene**

  Der Bericht enthält Daten von sekundären und virtuellen Administrationsservern, die sich unter dem aktuellen Administrationsserver auf der Verschachtelungsebene befinden, die kleiner oder gleich dem angegebenen Wert ist.

  Als Standardwert ist 1 vorgegeben. Sie sollten diesen Wert ändern, wenn Sie Informationen von sekundären Administrationsservern sammeln müssen, die sich auf niedrigeren Ebenen in der Struktur befinden.

- **Intervall zum Warten auf Daten (Min.)**

  Vor Erstellen des Berichts wartet der Administrationsserver, für den die Berichtsvorlage erstellt wurde, während der angegebenen Anzahl von Minuten auf Daten von sekundären Administrationsservern. Wenn nach Ablauf dieses Zeitraums keine Daten von einem sekundären Administrationsserver eingehen, wird der Bericht dennoch ausgeführt. Anstelle der eigentlichen Daten zeigt der Bericht Daten aus dem Cache (wenn die Option **Daten von sekundären Administrationsservern im Cache zwischenspeichern** aktiviert ist) oder **N/A** (nicht verfügbar).

  Der Standardwert beträgt 5 (Minuten).

- **Daten von sekundären Administrationsservern im Cache zwischenspeichern**

  Sekundäre Administrationsserver übertragen regelmäßig Daten an den Administrationsserver, für den die Berichtsvorlage erstellt wird. Dort werden die übertragenen Daten im Cache gespeichert.

  Wenn der aktuelle Administrationsserver beim Erstellen des Berichts keine Daten von einem sekundären Administrationsserver empfangen kann, zeigt der Bericht Daten aus dem Cache an. Das Datum, an dem die Daten in den Cache übertragen wurden, wird ebenfalls angezeigt.

  Wenn Sie diese Option aktivieren, können Sie die Daten von sekundären Administrationsservern anzeigen, auch wenn die aktuellen Daten nicht mehr abgerufen werden können. Die angezeigten Daten können jedoch veraltet sein.

  Diese Option ist standardmäßig deaktiviert.

- **Häufigkeit des Cache-Updates (Std.)**

  Sekundäre Administrationsserver übertragen in regelmäßigen Abständen Daten an den Administrationsserver, für den die Berichtsvorlage erstellt wird. Sie können diesen Zeitraum in Stunden angeben. Wenn Sie 0 Stunden angeben, werden die Daten nur übertragen, wenn der Bericht generiert wird.

  Als Standardwert ist 0 vorgegeben.

- **Detaillierte Informationen von sekundären Administrationsservern übertragen**

  Im generierten Bericht enthält die Tabelle mit den detaillierten Berichtsdaten Daten von sekundären Administrationsservern des Administrationsservers, für den die Berichtsvorlage erstellt wird.

  Wenn Sie diese Option aktivieren, wird die Berichtserstellung verlangsamt und der Datenverkehr zwischen den Administrationsservern erhöht. Sie können jedoch alle Daten in einem Bericht anzeigen.

  Anstatt diese Option zu aktivieren, möchten Sie möglicherweise detaillierte Berichtsdaten analysieren, um einen fehlerhaften sekundären Administrationsserver zu erkennen und dann denselben Bericht nur für den fehlerhaften Administrationsserver zu generieren.

  Diese Option ist standardmäßig deaktiviert.

- Registerkarte **Felder**

  Wählen Sie die im Bericht anzuzeigenden Felder und verwenden Sie die Schaltflächen **Nach oben** und **Nach unten**, um die Reihenfolge dieser Felder zu ändern. Verwenden Sie die Schaltflächen **Hinzufügen** oder **Bearbeiten**, um festzulegen, ob die Informationen im Bericht nach den jeweiligen Feldern sortiert und gefiltert werden müssen.

  Im Abschnitt **Filter der Detail-Felder** können Sie auch auf die Schaltfläche **Filter konvertieren** klicken, um die Verwendung des erweiterten Filterformats zu starten. Mit diesem Format können Sie die in verschiedenen Feldern angegebenen Filterbedingungen mithilfe der logischen ODER-Verknüpfung kombinieren. Nach dem Klicken auf die Schaltfläche wird rechts das Bedienfeld **Filter konvertieren** geöffnet. Klicken Sie auf die Schaltfläche **Filter konvertieren**, um die Konvertierung zu bestätigen. Sie können jetzt einen konvertierten Filter mit Bedingungen aus dem Abschnitt **Detail-Felder** definieren, die mithilfe der logischen ODER-Verknüpfung angewendet werden.

  > Durch die Konvertierung eines Berichts in das Format zur Unterstützung komplexer Filterbedingungen, wird der Bericht inkompatibel zu den vorherigen Versionen von Kaspersky Security Center (11 und früher). Außerdem enthält der konvertierte Bericht keine Daten von sekundären Administrationsservern mit diesen inkompatiblen Versionen.

5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

6. Schließen Sie das Fenster **Bericht <Berichtsname> bearbeiten**.

Der aktualisierte Bericht wird in der Liste der Berichtsvorlagen angezeigt.

Einen Bericht in eine Datei exportieren

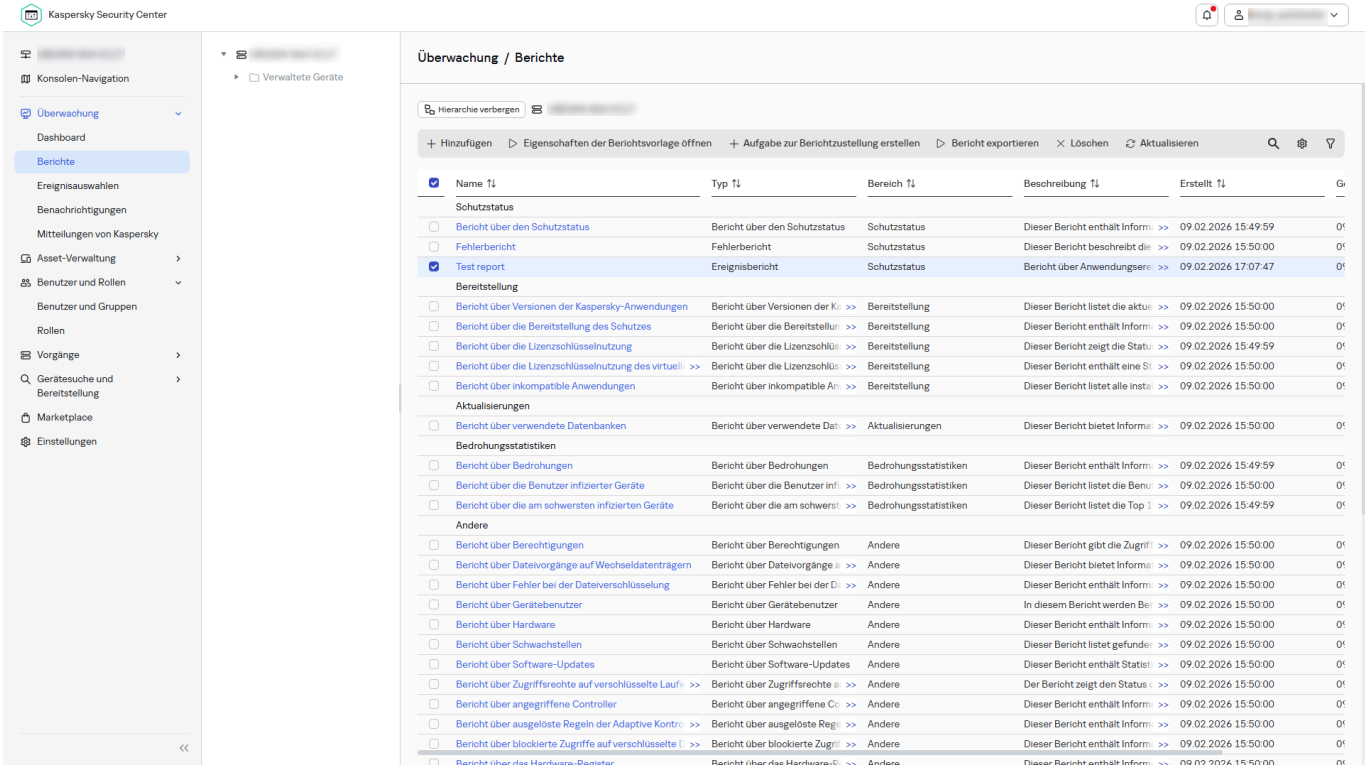
Sie können einen oder mehrere Berichte im xml-, html- oder pdf-Format speichern. Mit Kaspersky Security Center Linux können Sie bis zu 10 Berichte gleichzeitig in Dateien mit dem angegebenen Format exportieren.

So exportieren Sie einen Bericht in eine Datei:

1. Wechseln Sie im Hauptmenü zu **Überwachung → Berichte**.

2. Wählen Sie die Berichte aus, die Sie exportieren möchten.

   Wenn Sie mehr als 10 Berichte auswählen, wird die Schaltfläche **Bericht exportieren** deaktiviert.



Die Liste der Berichte

3. Klicken Sie auf die Schaltfläche **Bericht exportieren**.

4. Passen Sie im nächsten Fenster folgende Exporteinstellungen an:

   - **Dateiname**.

     Wenn Sie einen Bericht zum Exportieren auswählen, geben Sie den Dateinamen des Berichts an.

     Wenn Sie mehr als einen Bericht auswählen, stimmen die Namen der Berichtsdateien mit den Namen der ausgewählten Berichtsvorlagen überein.

   - **Maximale Anzahl an Einträgen**.

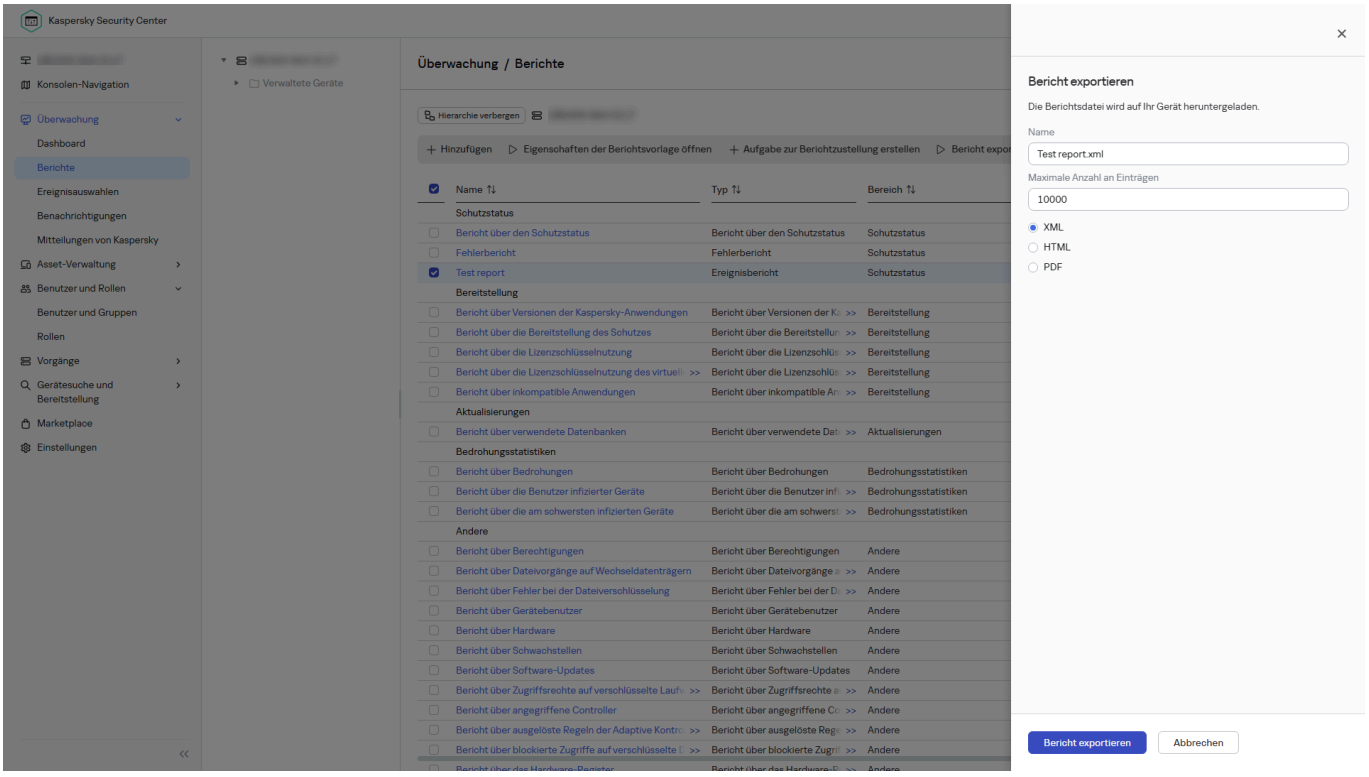
     Geben Sie die maximale Anzahl von Einträgen an, die in der Berichtsdatei enthalten sein sollen. Als Standardwert ist 10.000 vorgegeben.

     Einen Bericht kann mit einer unbegrenzten Anzahl von Einträgen exportiert werden. Beachten Sie, dass sich der Zeitaufwand für das Generieren und Exportieren des Berichts erhöht, wenn der Bericht eine große Anzahl von Einträgen enthält.

   - **Dateiformat**.

     Wählen Sie das Dateiformat für den Bericht aus: XML, HTML oder PDF. Wenn Sie mehrere Berichte exportieren, werden alle ausgewählten Berichte im angegebenen Format als separate Dateien gespeichert.

Um einen Bericht ins PDF-Format zu konvertieren, wird das Tool wkhtmltopdf benötigt. Wenn Sie die Option PDF auswählen, überprüft der Administrationsserver, ob das Tool wkhtmltopdf auf dem Gerät installiert ist. Ist das Tool nicht installiert, meldet die Anwendung, dass dieses Tool auf dem Administrationsserver-Gerät installiert werden muss. Installieren Sie das Tool manuell und gehen Sie dann zum nächsten Schritt.



Angeben der Exporteinstellungen des Berichts

5. Klicken Sie auf die Schaltfläche **Bericht exportieren**.

Der Bericht wird in einer Datei mit angegebenen Format gespeichert.

Bericht erstellen und anzeigen

Um einen Bericht zu erstellen und anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung** → **Berichte**.

2. Klicken Sie auf den Namen der Berichtsvorlage, die Sie zum Erstellen eines Berichts verwenden möchten.

   Ein Bericht, der die ausgewählte Vorlage verwendet, wird erstellt angezeigt.

Berichtsdaten werden gemäß der für den Administrationsserver eingestellten Lokalisierung angezeigt.

In den generierten Berichten werden einige Schriftarten in den Diagrammen möglicherweise falsch angezeigt. Um dieses Problem zu beheben, installieren Sie die Bibliothek "fontconfig". Überprüfen Sie bitte außerdem, ob die Fonts, die der Lokalisierungseinstellung Ihres Betriebssystems entsprechen auch im Betriebssystem installiert sind.

Im Bericht werden folgende Daten angezeigt:

- Auf der Registerkarte **Übersicht**:
  - Typ und Name des Berichts, eine Kurzbeschreibung und der Berichtszeitraum sowie Informationen darüber, für welche Gerätegruppe der Bericht erstellt wurde.
  - Graph-Diagramm mit den repräsentativsten Berichtsdaten.
  - Übersichtstabelle mit Kennziffern des Berichts.
- Auf der Registerkarte **Details** wird eine Tabelle mit detaillierten Berichtsdaten angezeigt.

Aufgabe zum Berichtsversand anlegen

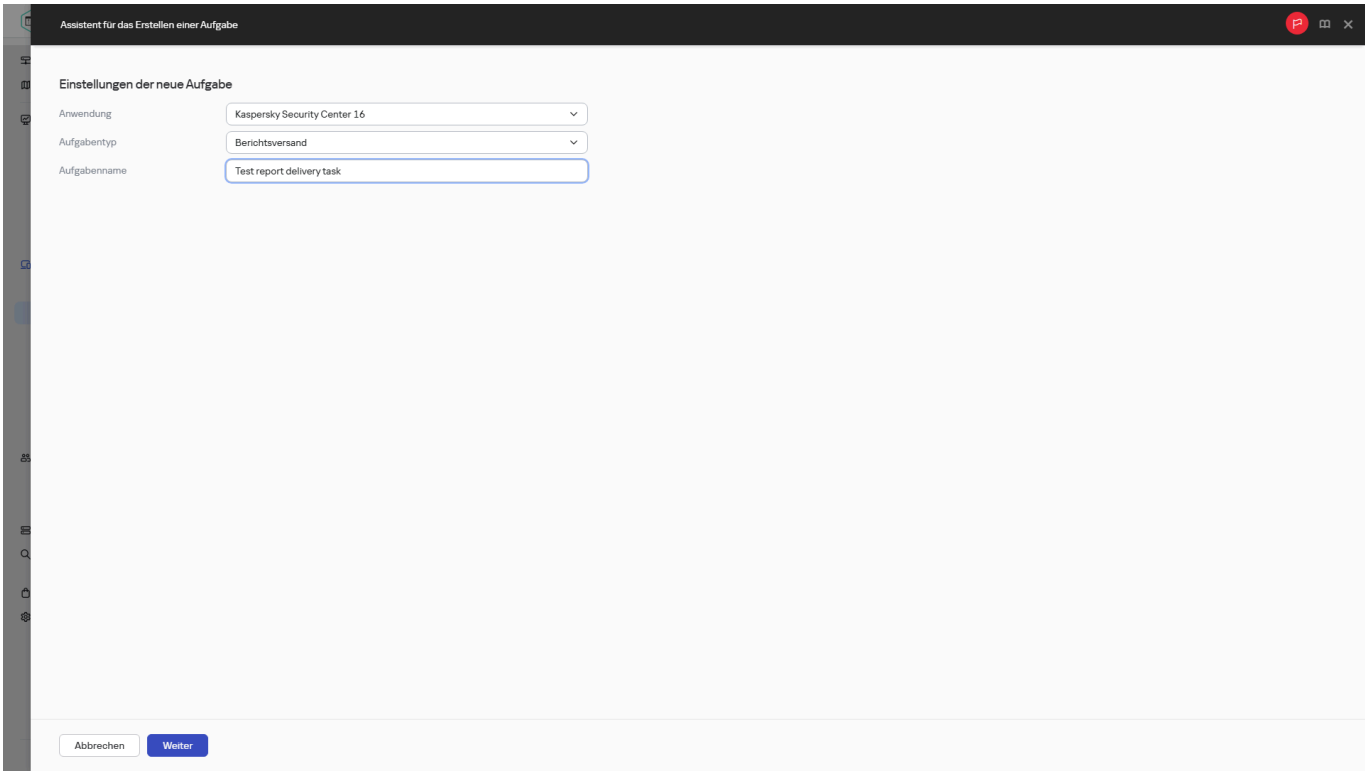
Sie könne eine Aufgabe erstellen, welche die ausgewählten Berichte versendet.

Um eine Aufgabe zum Versand von Berichten zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung** → **Berichte**.
2. Aktivieren Sie die Kontrollkästchen neben den Berichtsvorlagen, für die Sie eine Aufgabe zum Versand von Berichten erstellen möchten.
3. Klicken Sie auf die Schaltfläche **Aufgabe zur Berichtzustellung erstellen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.
4. Geben Sie im Schritt **Einstellungen der neue Aufgabe** des Assistenten den Namen der Aufgaben ein.

   Der Standardname lautet **Berichtsversand.** Wenn eine Aufgabe mit diesem Namen bereits existiert, wird dem Aufgabennamen eine laufende Nummer (<N>) hinzugefügt.



5. Geben Sie im Schritt **Berichtskonfiguration** des Assistenten die folgenden Einstellungen an:

   a. Berichtsvorlagen, welche die Aufgabe versenden soll.

   b. Format der Berichte: HTML, XLS oder PDF.

      Um einen Bericht ins PDF-Format zu konvertieren, wird das Tool wkhtmltopdf benötigt. Wenn Sie die Option PDF auswählen, überprüft der Administrationsserver, ob das Tool wkhtmltopdf auf dem Gerät installiert ist. Ist das Tool nicht installiert, meldet die Anwendung, dass dieses Tool auf dem Administrationsserver-Gerät installiert werden muss. Installieren Sie das Tool manuell und gehen Sie dann zum nächsten Schritt.

   c. Ob die Berichte per E-Mail gesendet werden sollen; welche Einstellungen für die Benachrichtigung per E-Mail verwendet werden sollen.

      Sie können bis zu 20 E-Mail-Adressen angeben. Mit der **Eingabetaste** können Sie E-Mail-Adressen voneinander separieren. Sie können auch eine durch Kommas getrennte Liste mit E-Mail-Adressen einfügen und anschließend die **Eingabetaste** drücken.

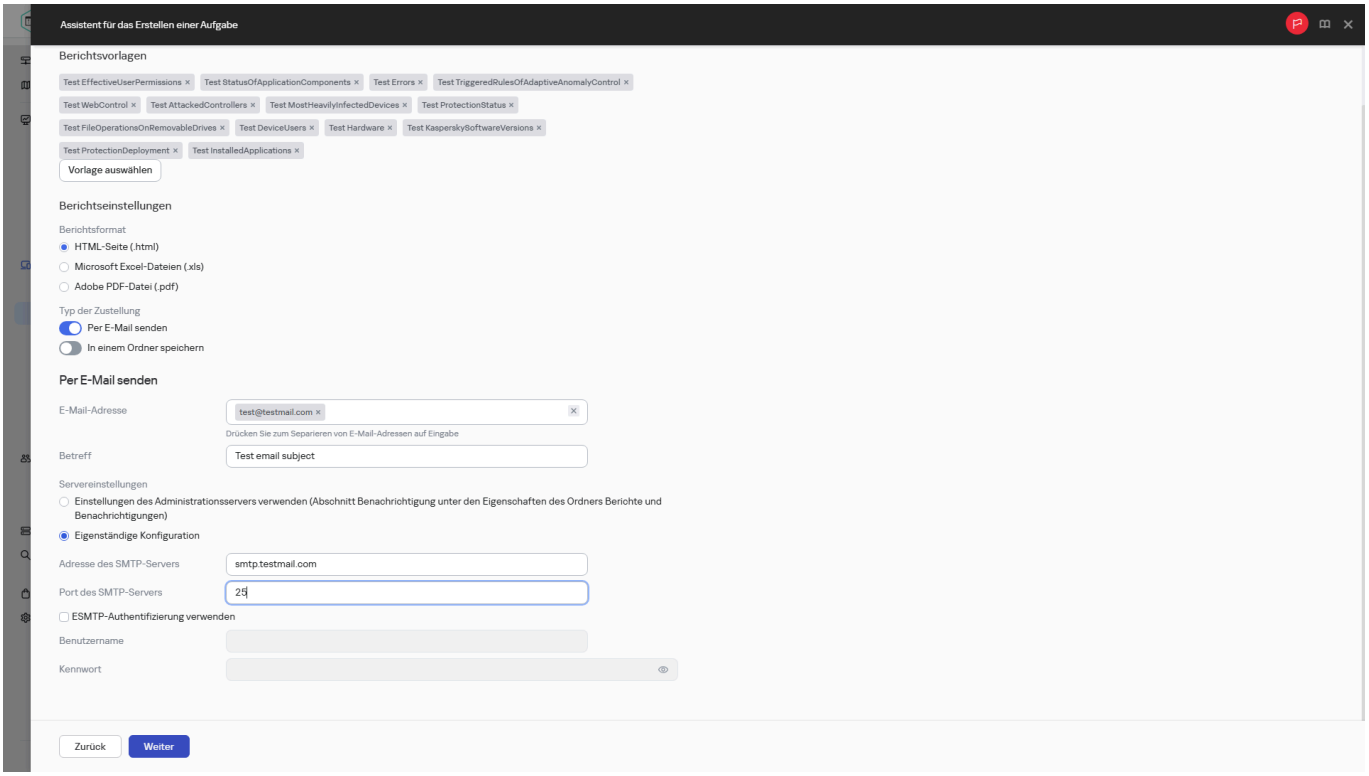
   d. Ob die Berichte mit den dazugehörigen Einstellungen in einem Ordner gespeichert werden sollen.

      Wenn Sie die Option **In einem Ordner speichern** aktivieren, müssen Sie einen POSIX-Pfad zu dem Ordner angeben. Wenn Sie die Berichte in einem freigegebenen Ordner speichern möchten, müssen Sie außerdem das Kontrollkästchen **Benutzerkonto für den Zugriff auf den freigegebenen Ordner angeben** aktivieren und anschließend das Benutzerkonto und das Kennwort für den Zugriff auf diesen Ordner angeben.

      > Wenn Sie die Berichte in einem freigegebenen Ordner speichern möchten, müssen Sie sicherstellen, dass für das Gerät mit installiertem Administrationsserver der Zugriff auf diesen Ordner eingerichtet ist. Wie und mit welchen Tools die Zugriffssicherung umgesetzt wird, ist von Ihrer Infrastruktur abhängig.

      Wenn Sie die Berichte in einem lokalen Ordner speichern, sind normalerweise keine Anmeldeinformationen erforderlich: Das Konto, unter dem der Administrationsserver ausgeführt wird, sollte bereits Zugriff auf diesen Ordner haben. Bei Bedarf können Sie in dem Assistenten im Schritt **Benutzerkonto für die Ausführung der Aufgabe auswählen** die Anmeldeinformationen eines Benutzers angeben.

Unabhängig von Ihrer Ordnerauswahl können Sie auch das Kontrollkästchen **Existierende Berichte vom gleichen Typ ersetzen** aktivieren. In diesem Fall überschreibt die neue Berichtsdatei die bei der vorherigen Aufgabenausführung im Ordner gespeicherte Berichtsdatei.



Angeben der Aufgabeneinstellungen

6. Wählen Sie im Schritt **Aufgabenzeitplan anpassen** des Assistenten den Startzeitplan für die Aufgabe aus.

   Die folgende Varianten sind für den Aufgabenzeitplan verfügbar:

   - **Manuell**

     Die Aufgabe wird nicht automatisch ausgeführt. Sie können diese nur manuell starten.

     Diese Variante ist standardmäßig ausgewählt.

   - **Alle n Minuten**

     Die Aufgabe wird ab der festgelegten Uhrzeit am Tag, an dem die Aufgabe erstellt wird, regelmäßig im festgelegten Intervall in Minuten ausgeführt.

     Standardmäßig wird die Aufgabe ab der aktuellen Systemzeit alle 30 Minuten ausgeführt.

   - **Alle n Stunden**

     Die Aufgabe wird ab dem angegebenen Datum und der Uhrzeit regelmäßig im angegebenen Intervall in Stunden ausgeführt.

     Die Aufgabe wird standardmäßig alle 6 Stunden ausgeführt, ausgehend von aktuellem Datum und aktueller Uhrzeit des Systems.

   - **Alle n Tage**

     Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. Zusätzlich können Sie ein Datum und eine Uhrzeit für den ersten Aufgabenstart angeben. Diese Zusatzoptionen sind verfügbar, wenn Sie von der Anwendung unterstützt werden, für welche Sie die Aufgabe erstellen.

     Standardmäßig wird die Aufgabe ab aktuellem Systemdatum und -uhrzeit täglich ausgeführt.

- **Alle n Wochen**

  Die Aufgabe wird regelmäßig im festgelegten wöchentlichen Intervall, an dem festgelegten Wochentag und zur festgelegten Uhrzeit, ausgeführt.

  Standardmäßig wird die Aufgabe jeden Freitag zur aktuellen Systemzeit ausgeführt.

- **Monatlich**

  Die Aufgabe wird regelmäßig am festgelegten Tag des Monats zur festgelegten Uhrzeit ausgeführt.

  In Monaten, die nicht über den festgelegten Tag verfügen, wird die Aufgabe am letzten Tag ausgeführt.

  Standardmäßig wird die Aufgabe am ersten Tag jeden Monats zur aktuellen Systemzeit ausgeführt.

- **An angegebenen Tagen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig beträgt die Startzeit 18:00 Uhr und es sind keine Tage des Monats ausgewählt.

  > Beachten Sie, dass Sie weder ein bestimmtes Datum im Monat noch die Nummer der Woche (erste, zweite Woche des Monats) auswählen, sondern die laufende Nummer des Wochentages innerhalb eines Monats. Wenn Sie den Cursor beispielsweise in die Zelle **Die** der **Erste** Zeile setzen, bedeutet dies, dass die Aufgabe jeden ersten Dienstag im neuen Monat ausgeführt wird.

  Sie können mehrere Wochentage auswählen.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Anwendungstypen aus, die Virenangriffe überwachen. Es sind folgende Anwendungstypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Anwendungstypen ausgewählt.

  Sie können abhängig von der Sicherheitsanwendung, die einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Anwendungstypen, die Sie nicht benötigen.

- **Nach Abschluss einer anderen Aufgabe**

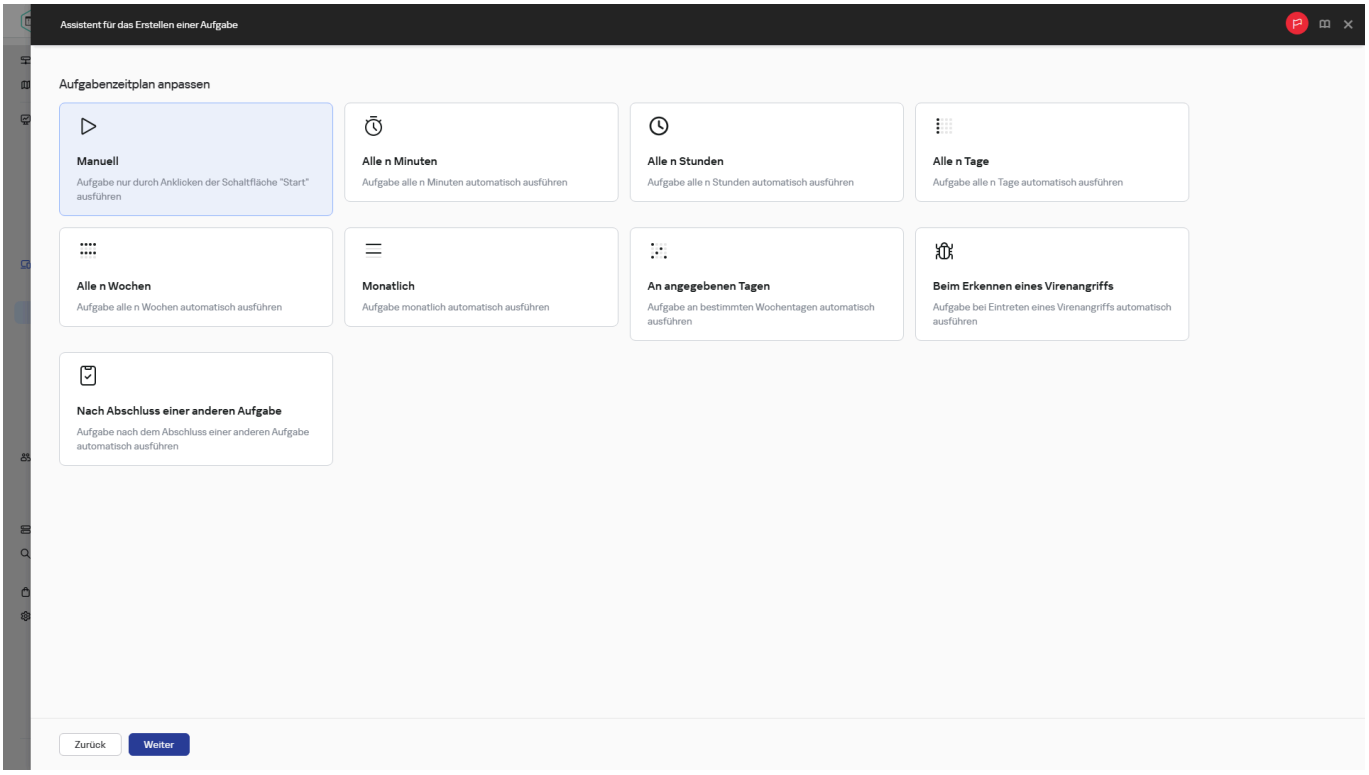
  Die aktuelle Aufgabe wird gestartet, nachdem eine andere Aufgabe abgeschlossen ist. Diese Option ist nur aktiv, wenn beide Aufgaben denselben Geräten zugewiesen sind. Sie können zum Beispiel die *Aufgabe zur Geräteverwaltung* mit der Option **Gerät einschalten** ausführen und, nachdem diese abgeschlossen ist, als auslösende Aufgabe die *Aufgabe zur Untersuchung auf Viren* starten.

  Sie müssen aus der Tabelle die auslösende Aufgabe und den Status auswählen, mit dem diese Aufgabe abgeschlossen werden soll (**Erfolgreich beendet** oder **Fehlgeschlagen**).

Bei Bedarf können Sie die Aufgaben in der Tabelle wie folgt suchen, sortieren und filtern:

- Geben Sie den Aufgabennamen in das Suchfeld ein, um die Aufgabe nach ihrem Namen zu suchen.
- Klicken Sie auf das Sortiersymbol, um die Aufgaben nach Namen zu sortieren.

  Standardmäßig werden die Aufgaben in alphabetischer Reihenfolge aufsteigend sortiert.
- Klicken Sie auf das Filtersymbol, filtern Sie im neuen Fenster die Aufgaben nach Gruppen und klicken Sie anschließend auf die Schaltfläche **Übernehmen**.



Auswählen des Zeitplans für den Aufgabenstart

7. Passen Sie in diesem Schritt des Assistenten die weiteren Einstellungen für den Aufgabenzeitplan an:

- Überprüfen oder ändern Sie im Abschnitt **Aufgabenzeitplan** den zuvor ausgewählten Zeitplan und passen Sie bei Bedarf das Zeitintervall, die Tage des Monats oder die Woche, sowie die Bedingung "Virenangriff" oder das Ausführen einer anderen Aufgabe als Auslöser für den Aufgabenstart an. Wenn ein passender Zeitplan ausgewählt ist, kann in diesem Abschnitt auch eine Startzeit angegeben werden.
- Geben Sie im Abschnitt **Zusätzliche Einstellungen** die folgenden Einstellungen an:
  - **Übersprungene Aufgaben starten**

    Diese Option bestimmt das Verhalten einer Aufgabe, falls ein Client-Gerät im Netzwerk nicht sichtbar ist, wenn die Aufgabe gestartet werden soll.

    Wenn diese Option aktiviert ist, versucht das System, die Aufgabe bei der nächsten Ausführung der Kaspersky-Anwendung auf dem Client-Gerät zu starten. Für den Aufgabenzeitplan **Manuell**, **Einmal** oder **Sofort** wird die Aufgabe sofort gestartet, wenn das Gerät im Netzwerk sichtbar wird, oder sofort, nachdem das Gerät in den Aufgabenbereich aufgenommen wird.

    Wenn diese Option deaktiviert ist, werden nur geplante Aufgaben auf den Client-Geräten ausgeführt. Für die Optionen **Manuell**, **Einmal** und **Sofort** des Zeitplans werden die Aufgaben nur auf den Geräten ausgeführt, die im Netzwerk sichtbar sind. Sie können diese Option zum Beispiel für eine ressourcenintensive Aufgabe deaktivieren, die sie nur außerhalb der Geschäftszeiten ausführen möchten.

Diese Option ist standardmäßig deaktiviert.

- **Automatische zufällige Verzögerung für Aufgabenstarts verwenden**

  Wenn diese Option aktiviert ist, wird die Aufgabe zufällig innerhalb eines festgelegten Zeitintervalls gestartet (*verteilter Aufgabenstart*). Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Die verteilte Startzeit wird automatisch beim Erstellen der Aufgabe berechnet, abhängig von der Anzahl der Client-Geräte, für welche die Aufgabe bestimmt wurde. Danach wird die Aufgabe immer zur berechneten Startzeit gestartet. Wenn die Aufgabeneinstellungen jedoch bearbeitet werden oder die Aufgabe manuell gestartet wird, ändert sich der berechnete Wert für den Zeitraum für den Aufgabenstart.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

- **Automatische zufällige Verzögerung des Aufgabenstarts innerhalb eines Intervalls von**

  Wenn diese Option aktiviert ist, wird die Aufgabe auf Client-Geräten zufällig innerhalb des festgelegten Zeitintervalls gestartet. Ein verteilter Aufgabenstart verhindert den gleichzeitigen Zugriff einer großen Anzahl von Client-Geräten auf den Administrationsserver beim Start einer Aufgabe nach Zeitplan.

  Wenn diese Option deaktiviert ist, erfolgt der Aufgabenstart auf den Client-Geräten gemäß dem Zeitplan.

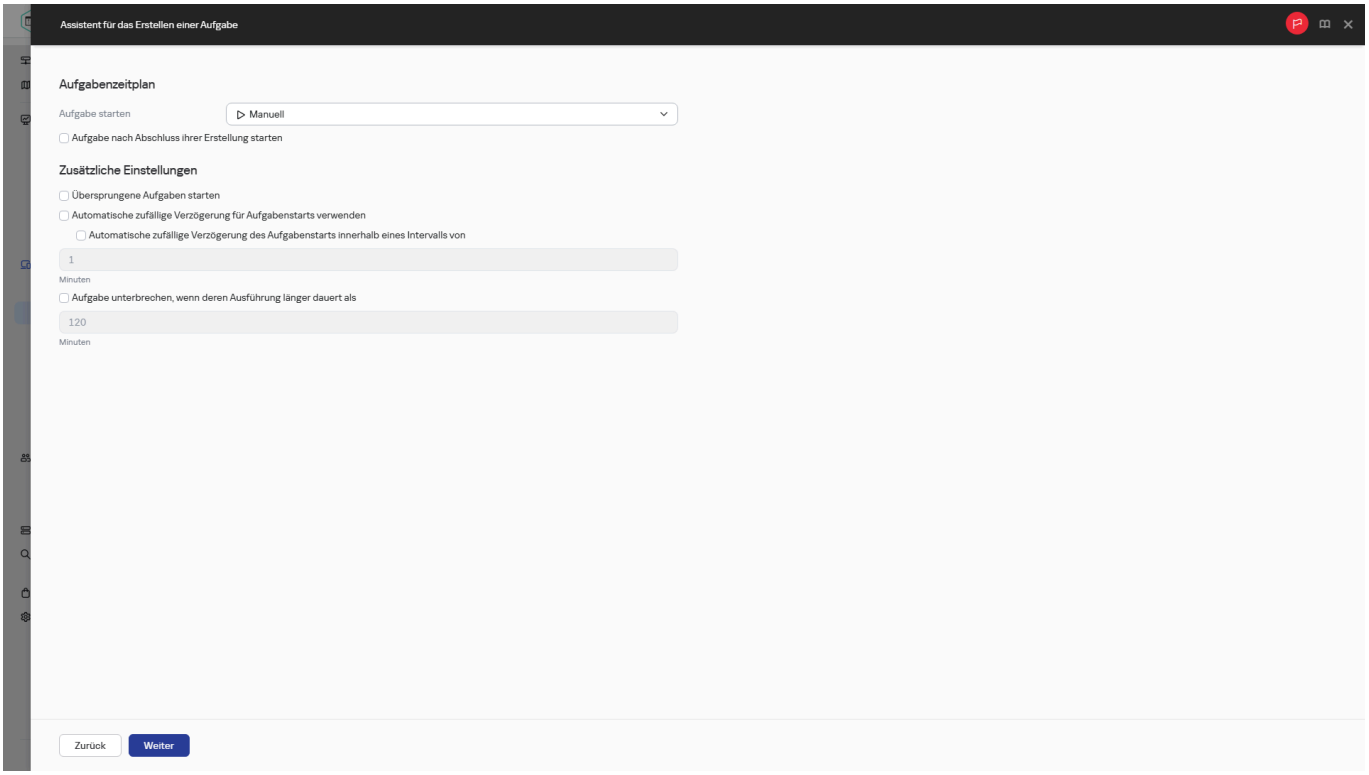
  Diese Option ist standardmäßig deaktiviert. Standardmäßig beträgt der Zeitraum eine Minute.

- **Aufgabe unterbrechen, wenn deren Ausführung länger dauert als**

  Nachdem die festgelegte Zeitspanne abgelaufen ist, wird die Aufgabe automatisch angehalten, egal ob sie abgeschlossen ist oder nicht.

  Aktivieren Sie diese Option, wenn Sie Aufgaben, deren Ausführung zu lange dauert, unterbrechen (oder anhalten) möchten.

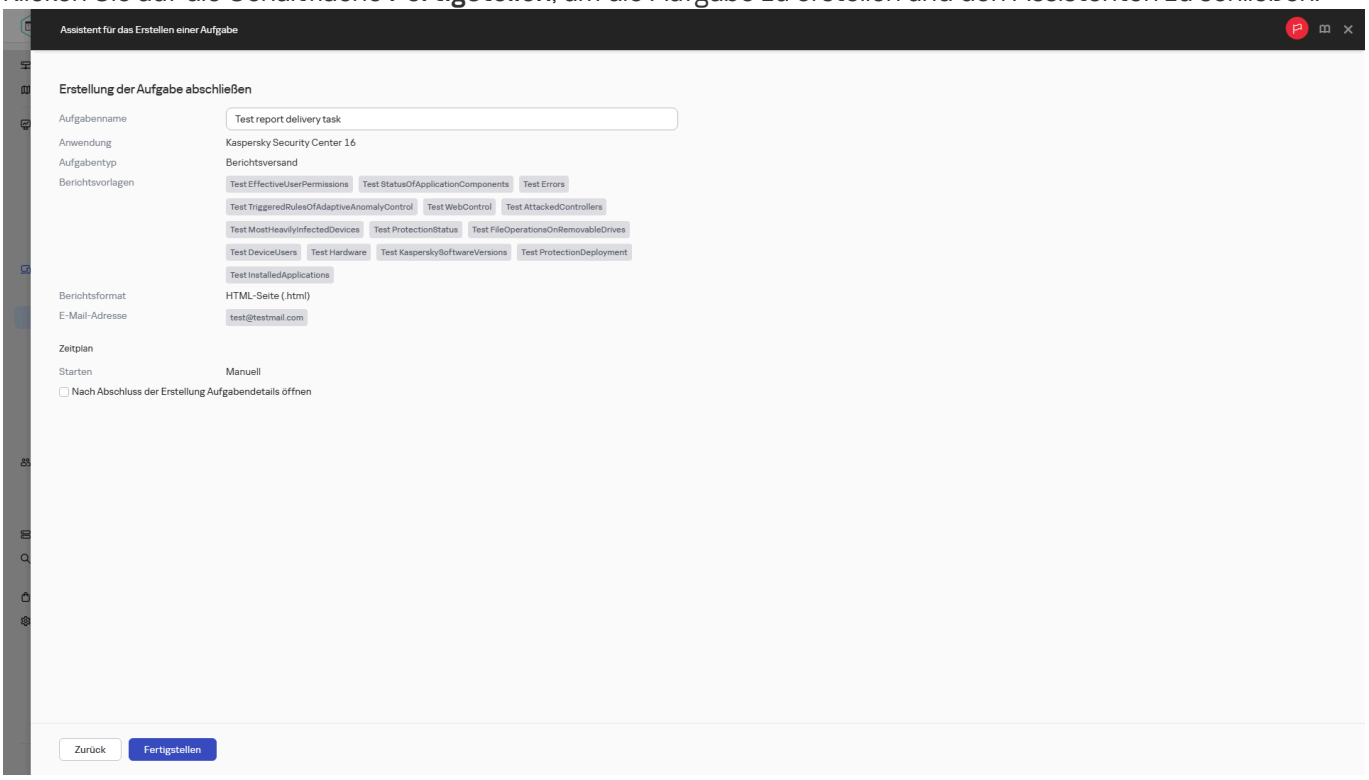
  Diese Option ist standardmäßig deaktiviert. Die Standardzeit für die Aufgabenausführung beträgt 120 Minuten.



8. Geben Sie im Schritt **Benutzerkonto für die Ausführung der Aufgabe auswählen** des Assistenten die Anmeldeinformationen des Benutzerkontos an, unter dem die Aufgabe ausgeführt werden soll.

9. Wenn Sie nach Erstellung der Aufgabe weitere Aufgabeneinstellungen bearbeiten möchten, aktivieren Sie auf in dem Schritt **Erstellung der Aufgabe abschließen** des Assistenten die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** (diese Option ist standardmäßig aktiviert).

10. Klicken Sie auf die Schaltfläche **Fertigstellen**, um die Aufgabe zu erstellen und den Assistenten zu schließen.



Abschließen der Aufgabenerstellung

Die Aufgabe für den Versand von Berichten wird erstellt. Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit den Aufgabeneinstellungen geöffnet.

Berichtsvorlagen löschen

Um eine oder mehrere Berichtsvorlagen zu löschen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Überwachung → Berichte**.

2. Aktivieren Sie die Kontrollkästchen neben den Berichtsvorlagen, die Sie löschen möchten.

3. Klicken Sie auf die Schaltfläche **Löschen**.

4. Klicken Sie im folgenden Fenster auf **OK**, um die Auswahl zu bestätigen.

Die ausgewählten Berichtsvorlagen werden gelöscht. Wenn diese Berichtsvorlagen in Aufgaben zum Berichtsversand verwendet wurden, werden sie auch aus den entsprechenden Aufgaben entfernt.

Schutzstufe anzeigen

Der Indikator für die Schutzstufe zeigt aktuelle Informationen über den Schutz Ihres Administrationsservers und der Verteilungspunkte an. Auf diese Weise können Sie die Implementierung des Härtungsleitfadens verfolgen. Der Indikator wird unter **Überwachung** → **Dashboard** angezeigt und kann nicht ausgeblendet oder in einem anderen Menüabschnitt der Web Console platziert werden. Wenn Sie auf den Indikator klicken, können Sie zum Abschnitt "Härtung der Infrastruktur" wechseln und den Status der Schutzparameter für den Administrationsserver und die Verteilungspunkte anzeigen. Um die Sicherheit Ihrer Infrastruktur zu erhöhen, müssen Sie die möglicherweise vorhandenen Probleme beheben.

Der Indikator kann einen der folgenden Statuswerte haben:

- Schutz ist konfiguriert.
- Schutz ist teilweise konfiguriert.
- Es ist kein Schutz konfiguriert.

So zeigen Sie detaillierte Informationen über die Schutzstufe an

Der Gesamtstatus des Indikators wird durch den Status der Schutzparameter gebildet.

Um die Parameter anzuzeigen, klicken Sie auf den Indikator.

Im neuen Fenster **Härtung der Infrastruktur** sind die Parameter nach geschützten Objekten gruppiert: Administrationsserver und Verteilungspunkte.

Jeder Schutzparameter wird abhängig von Ihren Zugriffsrechten in einem der folgenden Zustände angezeigt:

- ✅ – wenn keine Probleme zu beheben sind oder Sie nicht über die erforderlichen Zugriffsrechte verfügen.
- ⚠ oder ❌ – wenn Probleme zu beheben sind.

Die folgenden Parameter werden nur für den Administrationsserver angezeigt:

- Das Backup ist konfiguriert
- Die Wartung des Administrationsservers ist konfiguriert
- Die TLS-Verschlüsselung aktiviert

Die folgenden Parameter werden sowohl für den Administrationsserver als auch für die Verteilungspunkte angezeigt:

- Es ist Sicherheitsanwendung installiert
- Es wird Richtlinie angewendet
- Das Update der Antiviren-Datenbanken ist konfiguriert

Funktionen für den Administrationsserver:

- Alle Schutzparameter werden nur für den physischen Administrationsserver berechnet und nicht auf virtuelle Server angewendet.

  Wenn Sie über eine hierarchische Struktur aus mehreren Administrationsservern verfügen, wird der Indikator der Schutzstufe für jeden physischen Server separat berechnet.

- Die Parameter **Sicherheitsanwendung ist installiert**, **Richtlinie wird angewendet** und **Update der Antiviren-Datenbanken ist konfiguriert** werden für ein Gerät mit installiertem Administrationsserver berechnet.

- Im Falle eines bereitgestellten Failover-Clusters von Kaspersky Security Center Linux werden die Parameter **Sicherheitsanwendung ist installiert**, **Richtlinie wird angewendet** und **Update der Antiviren-Datenbanken ist konfiguriert** für jeden Knoten berechnet.

Berechnung des Indikatorstatus

Der Indikatorstatus wird wie in der Tabelle beschrieben berechnet.

Indikatorstatus	Bedingung
Der Schutz ist konfiguriert.	Alle Schutzparameter haben den Status ✓.
Der Schutz ist teilweise konfiguriert.	Der Parameter **Update der Antiviren-Datenbanken** hat den Status ⚠, während alle anderen Parameter den Status ✓ haben.
Es ist kein Schutz konfiguriert.	Wenn mindestens einer der folgenden Schutzparameter den Status ✗ hat.

Es ist Sicherheitsanwendung installiert

Mit Sicherheitsanwendungen können Sie Ihre Geräte vor verschiedenen Arten von Bedrohungen schützen, einschließlich Netzwerkangriffe, Phishing-Angriffe und betrügerische Angriffe.

Der Parameter wird mit dem Status ✓ angezeigt, wenn eine der Bedingungen erfüllt ist:

- Sie haben keine Zugriffsrechte auf die Geräte.

- Sie verfügen über die Berechtigung **Lesen** im Funktionsbereich **Allgemeine Funktionen → Basisfunktionen**, während auf den Geräten der Administrationsagent und eine Sicherheitsanwendung installiert sind.

  > Die Bedingung muss auf allen Geräten erfüllt sein, die Ihnen gemäß Ihren Zugriffsrechten zur Verfügung stehen. Ausnahmen bilden jene Geräte, auf denen eine Anwendung installiert ist, die keinen Antiviren-Schutz benötigt (z. B. ein gesichertes Betriebssystem); Geräte ohne installierten Administrationsagenten, sodass die Informationen über das Gerät erst vor weniger als 24 Stunden auf dem Administrationsserver erschienen sind; autonome Geräte, die vor mindestens 7 Tagen zum letzten Mal mit dem Administrationsserver verbunden waren.

Der Parameter wird mit dem Status ✗ angezeigt, wenn alle Bedingungen erfüllt werden.

Sie müssen auf die Schaltfläche **Geräte anzeigen** klicken und die in der Tabelle beschriebenen Aktionen für die angezeigten Geräte ausführen.

Bedingung	Lösung
Auf dem Gerät ist kein Administrationsagent installiert.	Installieren Sie den Administrationsagenten. Für das Gerät mit dem Administrationsserver besteht die einfachste Methode zur Installation des Administrationsagenten darin, ein autonomes Installationspaket zu verwenden.
Das Gerät befindet sich in der Gruppe **Nicht zugeordnete Geräte**	Verschieben Sie das Gerät in die Gruppe "Verwaltete Geräte" oder in deren Untergruppe.
Es wurden keine Sicherheitsanwendungen gefunden oder für die installierte Sicherheitsanwendung ist der Echtzeit-Schutz deaktiviert	Installieren Sie eine Sicherheitsanwendung. Die Anwendung übermittelt Informationen über den Schutzstatus an den Administrationsserver. Sie können den Schutzstatus eines Geräts im Abschnitt Geräteeinstellungen: **Allgemein** → **Gerätestatus** anzeigen. Auf dem Gerät mit dem Administrationsserver müssen Sie Kaspersky Endpoint Security für Linux installieren.

Es wird Richtlinie angewendet

Eine Richtlinie besteht aus einer Reihe von Einstellungen für Sicherheitsanwendungen, die auf eine Administrationsgruppe und deren Untergruppen angewendet werden.

Der Parameter wird mit dem Status angezeigt, wenn eine der Bedingungen erfüllt ist:

- Sie haben keine Zugriffsrechte auf die Geräte.
- Sie verfügen über die Berechtigung **Lesen** im Funktionsbereich **Allgemeine Funktionen** → **Basisfunktionen**, während auf Ihren Geräten eine Sicherheitsanwendung installiert ist und eine aktive Richtlinie dieser Sicherheitsanwendung auf den Geräten angewendet wird.

  Die Bedingung muss auf allen Geräten erfüllt sein, die Ihnen gemäß Ihren Zugriffsrechten zur Verfügung stehen. Ausnahmen bilden jene Geräte, auf denen eine Anwendung installiert ist, die keinen Antiviren-Schutz benötigt (z. B. ein gesichertes Betriebssystem); Geräte ohne installierten Administrationsagenten, sodass die Informationen über das Gerät erst vor weniger als 24 Stunden auf dem Administrationsserver erschienen sind; autonome Geräte, die vor mindestens 7 Tagen zum letzten Mal mit dem Administrationsserver verbunden waren.

Der Parameter wird mit dem Status angezeigt, wenn alle Bedingungen erfüllt werden.

Sie müssen auf die Schaltfläche **Geräte anzeigen** klicken und die in der Tabelle beschriebenen Aktionen für die angezeigten Geräte ausführen.

Bedingung	Lösung
Auf dem Gerät ist keine Sicherheitsanwendung installiert.	Stellen Sie sicher, dass das Gerät nicht in der Auswahl des Schutzparameters **Sicherheitsanwendung ist installiert** enthalten ist.

Es wird keine Richtlinie auf das Gerät angewendet.	Stellen Sie sicher, dass für die Administrationsgruppe, der das Gerät angehört, eine Richtlinie erstellt wurde. Wenn dies nicht der Fall ist, erstellen und aktivieren Sie die Richtlinie. Wenn dies der Fall ist, stellen Sie Folgendes sicher: • Die erstellte Richtlinie ist aktiv. Wenn nicht, aktivieren Sie die Richtlinie. • Der Status der Richtlinienverteilung hat den Wert **Erfolgreich angewendet**. Wenn der Status **Mit Fehler angewendet** lautet, muss das Problem auf der Seite der Sicherheitsanwendung behoben werden.

Das Update der Antiviren-Datenbanken ist konfiguriert

Da die Antiviren-Datenbanken Ihre Geräte vor Bedrohungen schützen, müssen Sie die Datenbanken auf den Geräten regelmäßig und zeitnah aktualisieren.

Der Parameter wird mit dem Status ✅ angezeigt, wenn eine der Bedingungen erfüllt ist:

- Sie haben keine Zugriffsrechte auf die Geräte.
- Wenn Sie über die Berechtigung Lesen im Funktionsbereich Allgemeine Funktionen → Basisfunktionen verfügen, werden die Antiviren-Datenbanken auf den Geräten aktualisiert.

  Die Bedingung muss auf allen Geräten erfüllt sein, die Ihnen gemäß Ihren Zugriffsrechten zur Verfügung stehen. Ausnahmen bilden jene Geräte, auf denen eine Anwendung installiert ist, die keinen Antiviren-Schutz benötigt (z. B. ein gesichertes Betriebssystem); Geräte ohne installierten Administrationsagenten, sodass die Informationen über das Gerät erst vor weniger als 24 Stunden auf dem Administrationsserver erschienen sind; autonome Geräte, die vor mindestens 7 Tagen zum letzten Mal mit dem Administrationsserver verbunden waren.

Der Parameter wird mit dem Status ⚠️ angezeigt, wenn das letzte Update der Antiviren-Datenbanken auf einem Gerät mindestens 3 Tage zurückliegt.

Der Parameter wird mit dem Status ❌ angezeigt, wenn das letzte Update der Antiviren-Datenbanken auf einem Gerät mindestens 7 Tage zurückliegt.

So beheben Sie diese Probleme:

1. Klicken Sie neben dem Parameter auf die Schaltfläche "Geräte anzeigen".
2. Führen Sie für die angezeigten Geräte die folgenden Aktionen aus:

   a. Stellen Sie sicher, dass die Verbindung zwischen dem Administrationsagenten und dem Administrationsserver hergestellt ist.

   Wenn dies nicht der Fall ist, finden Sie weitere Informationen dazu in folgenden Artikeln:

   Beheben von Problemen beim Update der Antiviren-Datenbanken von Kaspersky Endpoint Security für Linux

   Probleme beim Update der Antiviren-Datenbanken aus der Datenverwaltung des Kaspersky Security Center

b. Stellen Sie sicher, dass die Kaspersky-Anwendung, deren Antiviren-Datenbanken Sie überprüfen, nicht gestoppt ist.

   Wenn die Anwendung gestoppt ist, starten Sie sie.

c. Zeigen Sie auf dem Gerät die Fehler an, die nach dem Update aufgetreten sind.

Das Backup ist konfiguriert

Empfehlungen zur Datensicherung des Administrationsservers finden Sie unter Daten des Administrationsservers sichern, kopieren und wiederherstellen.

Der Parameter wird mit dem Status ✅ angezeigt, wenn eine der Bedingungen erfüllt ist:

- Sie haben keine Zugriffsrechte, um mit der Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers zu arbeiten.
- Sie verfügen über die Berechtigungen **Lesen, Schreiben** und **Ausführen** im Funktionsbereich **Allgemeine Funktionen → Vorgänge mit dem Administrationsserver** und das Backup ist konfiguriert und wird regelmäßig ausgeführt.

Der Parameter wird mit dem Status ❌ angezeigt, wenn mindestens eine der folgenden Bedingungen erfüllt ist.

Bedingung	Lösung
Die Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers ist nicht erstellt.	Erstellen Sie die Aufgabe.
Für die Aufgabe zum Anlegen eines Daten-Backups des Administrationsservers wurden die erforderlichen Einstellungen des Zeitplans nicht konfiguriert.	Legen Sie in der Aufgabe zur Wartung des Administrationsservers für die Einstellung **Aufgabe starten** einen Wert fest, der von **Beim Erkennen eines Virenangriffs** und **Manuell** abweicht.

Die Wartung des Administrationsservers ist konfiguriert

Durch die Wartung des Administrationsservers können Sie im Ordner des Administrationsservers Speicherplatz freigeben und die Größe der Datenbank reduzieren. Dies trägt zu einer beschleunigten Verarbeitung von Anfragen bei und erhöht die Gesamtstabilität des Systems.

Der Parameter wird mit dem Status ✅ angezeigt, wenn eine der Bedingungen erfüllt ist:

- Sie haben keine Zugriffsrechte, um mit der Aufgabe zur Wartung des Administrationsservers zu arbeiten.
- Sie verfügen über die Berechtigungen **Lesen, Schreiben** und **Ausführen** im Funktionsbereich **Allgemeine Funktionen → Vorgänge mit dem Administrationsserver**, während die Wartung des Administrationsservers konfiguriert und regelmäßig ausgeführt wird.

  Die Berechtigungen müssen auf der Ebene des Administrationsservers festgelegt werden.

Der Parameter wird mit dem Status ❌ angezeigt, wenn mindestens eine der folgenden Bedingungen erfüllt ist.

Bedingung	Lösung
Die Aufgabe zur Wartung des Administrationsservers ist nicht erstellt.	Erstellen Sie die Aufgabe.
Für die Aufgabe zur Wartung des Administrationsservers wurden die erforderlichen Einstellungen des Zeitplans nicht konfiguriert.	Legen Sie in der Aufgabe zur Wartung des Administrationsservers für die Einstellung **Aufgabe starten** einen Wert fest, der von **Beim Erkennen eines Virenangriffs** und **Manuell** abweicht.

Die TLS-Verschlüsselung aktiviert

Sie müssen sicherstellen, dass nur die Versionen 1.2 und 1.3 des TLS-Protokolls zulässig sind. Die Verwendung früherer Versionen führt zu ernsthaften Risiken für die Datensicherheit und macht Systeme anfällig für Angreifer.

Der Parameter wird mit dem Status angezeigt, wenn nur die Versionen 1.2 und 1.3 des TLS-Protokolls zulässig sind.

Der Parameter wird mit dem Status angezeigt, wenn veraltete TLS-Versionen vor 1.2 erlaubt sind.

Um das Problem zu beheben, müssen Sie das Flag `SrvUseStrictSslSettings` auf den Wert `4` oder `5` setzen.

Ereignisse und Ereignisauswahl

Dieser Abschnitt enthält Informationen zu Ereignissen und Ereignisauswahlen, zu den in den Komponenten von Kaspersky Security Center Linux auftretenden Ereignistypen, und zur Verwaltung der Blockierung häufiger Ereignisse.

Über Ereignisse in Kaspersky Security Center Linux

Kaspersky Security Center Linux ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Kaspersky-Anwendungen aufgetreten sind. Die Informationen über Ereignisse werden in der Administrationsserver-Datenbank gespeichert.

Ereignisse nach Typ

In Kaspersky Security Center Linux gibt es die folgenden Ereignistypen:

- Allgemeine Ereignisse. Diese Ereignisse kommen in allen verwalteten Kaspersky-Anwendungen vor. Als allgemeines Ereignis gilt beispielsweise das Ereignis Virenangriff. Allgemeine Ereignisse haben eine streng definierte Syntax und Semantik. Allgemeine Ereignisse werden beispielsweise in Berichten und auf Dashboards verwendet.
- Spezifische Ereignisse für verwaltete Kaspersky-Anwendungen. Jede verwaltete Kaspersky-Anwendung hat eine eigene Auswahl von Ereignissen.

Ereignisse nach Quelle

Sie können die vollständige Liste der Ereignisse anzeigen, die von einer Anwendung auf der Registerkarte **Konfiguration von Ereignissen** in der Anwendungsrichtlinie generiert werden können. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen.

Ereignisse können von den folgenden Anwendungen generiert werden:

- Komponenten von Kaspersky Security Center Linux:
  - Administrationsserver
  - Administrationsagent
- Verwaltete Kaspersky-Anwendungen

  Weitere Informationen zu den Ereignissen, die von verwalteten Kaspersky-Anwendungen generiert werden, finden Sie in der Dokumentation der entsprechenden Anwendung.

Ereignisse nach Ereigniskategorie

Jedes Ereignis hat eine eigene Ereigniskategorie. Je nach den Bedingungen des Auftretens, können dem Ereignis verschiedene Ereigniskategorien zugewiesen werden. Es sind vier Ereigniskategorien verfügbar:

- *Kritisches Ereignis* – ein Ereignis, das auf das Auftreten eines kritischen Problems hinweist, das zu Datenverlust, einer Ausführungsstörung oder einem kritischen Fehler führen kann.
- *Funktionsfehler* – ein Ereignis, das auf das Auftreten eines ernsten Problems, Fehlers oder einer Störung hinweist, welches während der Ausführung einer Anwendung oder Prozedur entstanden ist.
- *Warnung* – ein nicht unbedingt ernstes dem Ereignis, das jedoch auf die potentiell mögliche Entstehung eines Problems in der Zukunft hinweist. Meistens gehört die Mehrzahl der Ereignisse zu den Warnungen, wenn nach ihrem Auftreten die Ausführung der Anwendung ohne Datenverlust oder eingeschränkter Funktionalität wiederhergestellt werden kann.
- *Infomeldung* – Ereignis, das zwecks Information über das erfolgreiche Ausführen einer Operation, die korrekte Ausführung einer Anwendung oder den Abschluss einer Prozedur auftritt.

Für jedes Ereignis ist eine Speicherdauer festgelegt, die in Kaspersky Security Center Linux angezeigt oder geändert werden kann. Einige Ereignisse werden nicht standardmäßig in der Administrationsserver-Datenbank gespeichert, da die für sie definierte Speicherdauer gleich Null ist. In externe Systeme können nur jene Ereignisse exportieren, die mindestens einen Tag in der Administrationsserver-Datenbank gespeichert werden.

Ereignisse der Komponenten von Kaspersky Security Center Linux

Jede Komponente von Kaspersky Security Center Linux hat einen eigenen Satz von Ereignistypen. Dieser Abschnitt enthält eine Liste mit Ereignissen, die auf dem Kaspersky Security Center Administrationsserver und im Administrationsagenten auftreten können. Die Typen der Ereignisse, die in den Kaspersky-Anwendungen auftreten, sind in diesem Abschnitt nicht aufgeführt.

Für jedes Ereignis, das von einer Anwendung generiert werden kann, können Sie in der Anwendungsrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Datenstruktur der Beschreibungen von Ereignistypen

Zu jedem Ereignistyp werden der dargestellte Name, der Identifikator (ID), der alphabetische Code, die Beschreibung und die Standard-Speicherdauer angezeigt.

- **Dargestellter Name des Ereignistyps**. Dieser Text wird in Kaspersky Security Center Linux angezeigt, wenn Sie Ereignisse konfigurieren und wenn diese auftreten.
- **Ereignistyp-ID**. Dieser numerische Code wird verwendet, wenn Sie Ereignisse zwecks Ereignisanalyse mithilfe von Drittanbieter-Tools verarbeiten.
- **Ereignistyp** (alphabetischer Code). Dieser Code wird verwendet, wenn Sie Ereignisse mithilfe der in der Datenbank von Kaspersky Security Center Linux verfügbaren öffentlichen Ansichten durchsuchen und verarbeiten und wenn Ereignisse in ein SIEM-System exportiert werden.
- **Beschreibung**. Dieser Text beschreibt die Situationen, in denen ein Ereignis eintreffen kann, und gibt Hinweise auf weiteres Vorgehen.
- **Standard-Speicherdauer**. Das ist die Anzahl der Tage, die ein Ereignis in der Administrationsserver-Datenbank gespeichert bleibt und in der Liste der Ereignisse auf dem Administrationsserver angezeigt wird. Nach Ablauf dieses Zeitraums wird das Ereignis gelöscht. Wenn als Speicherdauer der Wert 0 angegeben ist, werden solche Ereignisse gefunden, aber nicht in der Liste der Ereignisse auf dem Administrationsserver angezeigt. Wenn Sie angegeben haben, dass solche Ereignisse im Ereignisprotokoll des Betriebssystems gespeichert werden sollen, finden Sie die Ereignisse hier.

  Sie können die Speicherdauer für Ereignisse ändern: Legen Sie die Speicherdauer für ein Ereignis fest.

Ereignisse des Administrationsservers

Dieser Abschnitt informiert über die Ereignisse, die sich auf den Administrationsserver beziehen.

Ereignisse des Administrationsservers: Kritisch

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Kritisch**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Das Zertifikat des Administrationsservers für mobile Geräte ist abgelaufen	6129	KLSRV_EV_SRV_CERT_EXPIRED_DN	Ereignisse dieser Art treten auf, wenn die Zertifikate des Administrationsservers für mobile Geräte und UEFI-Geräte ablaufen. Sie müssen das abgelaufene Zertifikat aktualisieren.	180 Tage
Audit: Export nach SIEM fehlgeschlagen	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Ereignisse dieser Art treten auf, wenn der Export von Ereignissen in das SIEM-System aufgrund eines Verbindungsfehlers mit dem SIEM-System fehlgeschlagen ist.	180 Tage
Das Gerät wird nicht mehr verwaltet	4111	KLSRV_HOST_OUT_CONTROL	Ereignisse dieser Art treten auf, wenn ein verwaltetes Gerät ist im Netzwerk sichtbar ist, es aber über einen bestimmten Zeitraum keine Verbindung zum Administrationsserver hergestellt hat. Finden Sie heraus, warum der Administrationsagent auf diesem Gerät nicht ordnungsgemäß ausgeführt wird. Mögliche Ursachen können Netzwerkprobleme oder das Entfernen des Administrationsagenten von diesem Gerät sein.	180 Tage
Gerätestatus - "Kritisch"	4113	KLSRV_HOST_STATUS_CRITICAL	Ereignisse dieser Art treten auf, wenn einem verwalteten Gerät der Status *Kritisch* zugewiesen wird. Sie können die Bedingungen anpassen, unter denen der Gerätestatus zu *Kritisch* wechselt.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die Lizenz läuft bald ab	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Ereignisse dieser Art treten auf, wenn das Ablaufdatum einer kommerziellen Lizenz näher rückt. Einmal am Tag überprüft Kaspersky Security Center Linux, ob sich das Ablaufdatum der Lizenz nähert. Veröffentlicht werden Ereignisse dieses Typs 30 Tage, 15 Tage, 5 Tage und 1 Tag vor dem Ablaufdatum der Lizenz. Die Anzahl der Tage kann nicht geändert werden. Wird der Administrationsserver an dem entsprechenden Tag vor dem Ablaufdatum der Lizenz deaktiviert, so wird das Ereignis erst am darauf folgenden Tag veröffentlicht. Wenn die kommerzielle Lizenz abläuft, stellt Kaspersky Security Center Linux nur grundlegende Funktionen bereit. Sie können auf dieses Ereignis folgendermaßen reagieren: • Vergewissern Sie sich, dass dem Administrationsserver ein Reserve-Lizenzschlüssel hinzugefügt wurde. • Wenn Sie ein Abonnement verwenden, stellen Sie sicher, dies zu Verlängern. Ein unbeschränktes Abonnement wird automatisch verlängert, falls der vereinbarte Betrag bis zum Fälligkeitsdatum an den Dienstleister überwiesen wird.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Lizenzbeschränkung wurde überschritten	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Kaspersky Security Center Linux überprüft einmal täglich, ob eine Lizenzbeschränkung überschritten wurde. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Beschränkungen der Lizenz durch Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind, überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinheiten die von einer Lizenz abgedeckten werden, 110% der von der Lizenz abgedeckten Gesamtzahl an Einheiten überschreitet. Auch wenn dieses Ereignis eintritt, werden die Client-Geräte geschützt. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie ungenutzte Geräte. • Stellen Sie eine Lizenz für weitere Geräte zur Verfügung (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). Kaspersky Security Center Linux ermittelt die Regeln zum Auslösen von Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Eingeschränkter Funktionsmodus	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Ereignisse dieser Art treten auf, wenn Kaspersky Security Center Linux beginnt, mit Grundlegenden Funktionen und ohne Schwachstellen- und Patch-Management sowie ohne Funktionalität "Mobile Geräte verwalten", zu arbeiten. Im Folgenden die Gründe für und geeignete Reaktionen auf das Ereignis: • Die Gültigkeitsdauer der Lizenz ist abgelaufen. Um den vollen Funktionsumfang von Kaspersky Security Center Linux zu nutzen, stellen Sie eine Lizenz bereit (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). • Der Administrationsserver verwaltet mehr Geräte, als in der Lizenz angegeben. Verschieben Sie die Geräte aus der Administrationsgruppe des Administrationsservers in die eines anderen Administrationsserver (wenn das Lizenzlimit des anderen Administrationsservers dies zulässt).	180 Tage
Das MDM-Zertifikat ist abgelaufen	4132	KLSRV_CERTIFICATE_EXPIRED	Ereignisse dieser Art treten auf, wenn auf mobilen Geräten das Client-Zertifikat abläuft.	180 Tage
Die Schlüsseldatei wurde der Deny-Liste hinzugefügt	4124	KLSRV_LICENSE_BLACKLISTED	Ereignisse dieser Art treten auf, wenn Kaspersky den von Ihnen verwendeten Aktivierungscode oder die Schlüsseldatei auf die Deny-Liste setzt. Kontaktieren Sie den Technischen Support für weitere Informationen.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die Modul-Updates der Kaspersky-Anwendung wurden widerrufen	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Ereignisse dieser Art treten auf, wenn nahtlose Updates von den Kaspersky-Experten zurückgerufen wurden (für diese Updates wird der Status *Zurückgerufen* angezeigt); zum Beispiel, wenn Updates auf eine neuere Version aktualisiert werden müssen. Dieses Ereignis betrifft Patches für Kaspersky Security Center Linux. Module von Anwendungen, die durch Kaspersky verwaltet werden, sind nicht betroffen. Das Ereignis gibt den Grund an, warum das nahtlose Update nicht installiert wurde.	180 Tage
Virenangriff	• 26 (für Schutz vor bedrohlichen Dateien) • 27 (für Schutz vor E-Mail-Bedrohungen) • 28 (für Firewall)	GNRL_EV_VIRUS_OUTBREAK	Ereignisse dieser Art treten auf, wenn auf mehreren verwalteten Geräten die Anzahl an erkannten schädlichen Objekten den Schwellwert innerhalb eines kurzen Zeitraums überschreitet. Sie können auf dieses Ereignis folgendermaßen reagieren: • Legen Sie den Schwellenwert in den Eigenschaften des Administrationsservers fest. • Erstellen Sie eine strengere Richtlinie, die aktiviert wird oder erstellen Sie eine Aufgabe, die bei Auftreten dieses Ereignisses ausgeführt wird.	

Ereignisse des Administrationsservers: Funktionsfehler

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Funktionsfehler**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Kopieren der Updates in den angegebenen Ordner nicht ausgeführt	4123	KLSRV_UPD_REPL_FAIL	Ereignisse dieser Art treten auf, wenn Programm-Updates in einen oder mehrere zusätzlich freigegebene Ordner kopiert werden. Sie können auf dieses Ereignis folgendermaßen reagieren: • Prüfen Sie, ob das Benutzerkonto, das für den Zugriff auf die Ordner verwendet wird, über Berechtigung zum Schreiben verfügt. • Prüfen Sie, ob sich der Benutzername und/oder das Kennwort zu diesen Ordnern geändert haben. • Überprüfen Sie die Internetverbindung, da sie die Ursache des Ereignisses sein kann. Folgen Sie den Anweisungen, um die Datenbanken und die Programm-Module zu aktualisieren.	180 Tage
Die Abfrage des Cloud-Segments konnte nicht ausgeführt werden	4143	KLSRV_KLCLOUD_SCAN_ERROR	Ereignisse dieser Art treten auf, wenn das Abfragen eines Netzwerksegments in der Cloud-Umgebung durch den Administrationsserver fehlschlägt. Studieren Sie die Informationen in der Ereignisbeschreibung und reagieren Sie entsprechend.	Wird nicht gespeichert
Für eine der lizenzierten Programmgruppen wurde die Beschränkung für die Anzahl von Installationen überschritten	4126	KLSRV_INVLICPROD_EXCEDED	Der Administrationsserver generiert Ereignisse dieser Art periodisch (stündlich). Ereignisse dieser Art treten auf, wenn Sie in Kaspersky Security Center Linux die Lizenzschlüssel von Drittanbieter-Anwendungen verwalten und wenn die Anzahl der Installationen das Limit überschreitet, das durch den Lizenzschlüssel der Drittanbieter-Anwendung festgelegt ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie Drittanbieter-Anwendungen von den Geräten, auf denen sie nicht verwendet werden. • Verwenden Sie eine Drittanbieter-Lizenz für mehr Geräte. Sie können die Lizenzschlüssel von Drittanbieter-Anwendungen verwalten, indem Sie die Funktionen der lizenzierten Anwendungsgruppe verwenden. Zur lizenzierten Anwendungsgruppe gehören Drittanbieter-Anwendungen, welche die von Ihnen festgelegten Kriterien erfüllen.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Kein freier Platz auf dem Datenträger	4107	KLSRV_DISK_FULL	Ereignisse dieser Art treten auf, wenn auf der Festplatte des Geräts, auf dem der Administrationsserver installiert ist, freier Speicherplatz knapp wird. Schaffen Sie freien Speicherplatz.	180 Tage
Kein freier Platz in der Administrationsserver-Datenbank	4110	KLSRV_DATABASE_FULL	Ereignisse dieser Art treten auf, wenn in der Administrationsserver-Datenbank kein freier Speicherplatz mehr vorhanden ist. Der Administrationsserver funktioniert nicht, wenn seine Datenbank die Kapazitätsgrenze erreicht hat und wenn weiteres Speichern in der Datenbank nicht möglich ist. Im Folgenden die Gründe für dieses Ereignis, in Abhängigkeit zu dem DBMS, dass Sie verwenden, sowie geeignete Reaktionen auf dieses Ereignis: • Begrenzung der Anzahl der Ereignisse, die in der Datenbank des Administrationsservers gespeichert werden sollen. • In der Administrationsserver-Datenbank befinden sich zu viele Ereignisse, die durch die Komponente "Programmkontrolle" gesendet wurden. Sie können die Einstellungen der Richtlinie in Kaspersky Endpoint Security, die sich auf die Speicherung von Ereignissen der Programmkontrolle in der Administrationsserver-Datenbank bezieht, ändern. Überprüfen Sie die Informationen zur Auswahl des DBMS.	180 Tage
Laufzeitfehler	4125	KLSRV_RUNTIME_ERROR	Ereignisse dieser Art treten bei unbekannten Problemen auf. Dabei handelt es sich meistens um DBMS-Probleme, Netzwerkprobleme und andere Hard- und Softwareprobleme. Informationen zu diesem Ereignis stehen in der Ereignisbeschreibung.	180 Tage
Kein Zugriff auf freigegebenen Ordner	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Ereignisse dieser Art treten auf, wenn der Freigegebene Ordner des Administrationsservers nicht verfügbar ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Überprüfen Sie, ob der Administrationsserver (auf dem sich der freigegebene Ordner befindet) angeschaltet und erreichbar ist. • Prüfen Sie, ob sich der Benutzername und/oder das Kennwort zu diesem Ordner geändert haben. • Prüfen Sie die Netzwerkverbindung.	180 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die Administrationsserver-Datenbank ist nicht verfügbar	4109	KLSRV_DATABASE_UNAVAILABLE	Ereignisse dieser Art treten auf, wenn die Administrationsserver-Datenbank nicht verfügbar ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Prüfen Sie, ob der Remote-Server mit dem installierten DBMS verfügbar ist. • Schauen Sie in die Protokolle des DBMS, um die Ursache für die Nichtverfügbarkeit der Administrationsserver-Datenbank zu finden.	180 Tage

Ereignisse des Administrationsservers: Warnung

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Warnung**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsservers: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Das Zertifikat des Administrationsservers für mobile Geräte läuft ab	6128	KLSRV_EV_SRV_CERT_EXPIRES_SOON	Ereignisse dieser Art treten auf, wenn die Zertifikate des Administrationsservers für mobile Geräte und UEFI-Geräte ablaufen. Sie müssen das abgelaufene Zertifikat aktualisieren.	90 Tage
Das APNs-Zertifikat läuft bald ab	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Ereignisse dieser Art treten auf, wenn das APNs-Zertifikat in weniger als 14 Tagen abläuft. Wenn das APNs-Zertifikat abläuft, müssen Sie manuell das APNs-Zertifikat erneuern und es auf einem iOS MDM-Server installieren. Es wird empfohlen, dass Sie den Zeitpunkt für das Erneuern des APNs-Zertifikats vor das Ablaufdatum legen.	Wird nicht gespeichert
Das APNs-Zertifikat ist abgelaufen	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Ereignisse dieser Art treten auf, wenn ein APNs-Zertifikat abläuft. Sie müssen manuell das APNs-Zertifikat erneuern und es auf einem iOS MDM-Server installieren.	Wird nicht gespeichert
Audit: testweise Verbindung zu SIEM-Server fehlgeschlagen	5120	KLAUD_EV_SIEM_TEST_FAILED	Ereignisse dieser Art treten auf, wenn ein automatischer Verbindungstest mit dem SIEM-Server fehlgeschlagen ist.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Zertifikat wurde entfernt	4134	KLSRV_CERTIFICATE_REMOVED	Ereignisse dieser Art treten auf, wenn ein Administrator ein Zertifikat beliebiger Art (General, Mail, VPN) für die Funktion "Verwaltung mobiler Geräte" entfernt. Nach dem Entfernen eines Zertifikats schlägt für die mobilen Geräte, die über dieses Zertifikat verbunden sind, die Verbindung mit dem Administrationsserver fehl. Dieses Ereignis kann hilfreich sein, wenn es darum geht, Fehlfunktionen im Zusammenhang mit der Verwaltung mobiler Geräte aufzuspüren.	90 Tage
Zertifikat wurde angefordert	4133	KLSRV_CERTIFICATE_REQUESTED	Ereignisse dieser Art treten auf, wenn das automatische Neuausstellen eines Zertifikats für die Funktion "Verwaltung mobiler Geräte" fehlschlägt. Im Folgenden werden die Ursachen für das Ereignis und angebrachte Reaktionen darauf ausgeführt: • Die automatische Neuausstellung wurde für ein Zertifikat initiiert, für das die Option **Zertifikat automatisch neu veröffentlichen, falls möglich** deaktiviert ist. Dies kann aufgrund eines Fehler geschehen, der bei der Erstellung des Zertifikats auftrat. Ein manuelles Neuausstellen des Zertifikats kann notwendig sein. • Wenn Sie eine Integration mit einer Public-Key-Infrastruktur verwenden, kann ein fehlendes Namensattribut des SAM-Benutzerkontos, welches für die PKI-Integration und zum Ausstellen der Zertifikate genutzt wird, die Ursache sein. Überprüfen Sie die Eigenschaften des Benutzerkontos.	90 Tage
Konflikt von Gerätenamen	4102	KLSRV_EVENT_HOSTS_CONFLICT	Ereignisse dieser Art treten auf, wenn der Administrationsserver zwei oder mehr verwaltete Geräte als ein Gerät wahrnimmt. Dies ist meistens dann der Fall, wenn ein geklontes Laufwerk für die Bereitstellung auf verwalteten Geräten verwendet wurde, und dabei der Administrationsagent auf einem Referenzgerät nicht in den dedizierten "Laufwerk klonen"-Modus versetzt wurde. Um diesen Fehler zu vermeiden, versetzen Sie den Administrationsagenten auf einem Referenzgerät in den "Laufwerk klonen"-Modus, bevor Sie das Laufwerk des Geräts klonen.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die Verbindung mit dem primären Administrationsserver wurde getrennt	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Ereignisse dieser Art treten auf, wenn die Verbindung zum primären Administrationsserver unterbrochen ist. Konsultieren Sie das Betriebssystem-Protokoll des Geräts, auf dem der primäre Administrationsserver installiert ist, und reagieren Sie entsprechend.	90 Tage
Die Verbindung mit dem sekundären Administrationsserver wurde getrennt	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Ereignisse dieser Art treten auf, wenn die Verbindung zum sekundären Administrationsserver unterbrochen ist. Konsultieren Sie das Betriebssystem-Protokoll des Geräts, auf dem der sekundäre Administrationsserver installiert ist, und reagieren Sie entsprechend.	90 Tage
Das Gerät war lange Zeit im Netzwerk inaktiv	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Ereignisse dieser Art treten auf, wenn ein verwaltetes Gerät für längere Zeit inaktiv erscheint. Dies ist meistens dann der Fall, wenn ein verwaltetes Gerät ausrangiert wurde. Sie können auf dieses Ereignis folgendermaßen reagieren: • Löschen Sie das Gerät manuell aus der Liste der verwalteten Geräte. Geben Sie mithilfe von Kaspersky Security Center Web Console den Zeitraum an, nach dessen Ablauf das Ereignis **Das Gerät war lange Zeit im Netzwerk inaktiv** erstellt wird. • Geben Sie mithilfe von Kaspersky Security Center Web Console den Zeitraum an, nach dessen Ablauf das Gerät automatisch aus der Gruppe entfernt wird.	90 Tage
Gerätestatus: "Warnung"	4114	KLSRV_HOST_STATUS_WARNING	Ereignisse dieser Art treten auf, wenn einem verwalteten Gerät der Status *Warnung* zugewiesen wird. Sie können die Bedingungen anpassen, unter denen der Gerätestatus zu *Warnung* wechselt.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Datei konnte nicht auf Gerät heruntergeladen werden	4165	KLSRV_FILE_DOWNLOAD_FAILED	Solche Ereignisse treten in auf, wenn: • Sie versuchen, eine Datei in den Unternehmenscontainer herunterzuladen, aber noch kein Unternehmenscontainer angelegt wurde. • auf dem Gerät nicht genügend Speicherplatz vorhanden ist. • die Informationen über die Datei nicht vom Server heruntergeladen werden konnten. • der Inhalt der Datei nicht vom Server heruntergeladen werden konnten. • der Ordner nicht auf dem Gerät erstellt werden konnte. • die Zugriffsberechtigung für die Datei auf dem persönlichen Gerät fehlt. • die Zugriffsberechtigung für die Datei in dem Unternehmenscontainer fehlt.	90 Tage
Die FCM-Nachricht konnte nicht an den FCM-Server gesendet werden	4140	KLSRV_GCM_GENERAL_ERROR	Ereignisse diese Art treten auf, wenn im Rahmen der Verwendung des Google Firebase Cloud Messaging HTTP-Protokolls unerwartete Fehler auf dem Administrationsserver auftreten. Studieren Sie die Informationen in der Ereignisbeschreibung und reagieren Sie entsprechend. Wenn Sie selbst keine Lösung für dieses Problem ausmachen können, ist es empfehlenswert den Technischen Support von Kaspersky zu kontaktieren.	90 Tage
Die FCM-Nachricht konnten nicht an das mobile Gerät gesendet werden	4138	KLSRV_GCM_DEVICE_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion "Verwaltung mobiler Geräte" so konfiguriert ist, dass sie Google Firebase Cloud Messaging (FCM) für die Verbindung verwalteter Geräte mit Android-Betriebssystem verwendet, und auf dem FCM-Server das Bearbeiten von empfangenen Administrationsserver-Anfragen fehlschlägt. Dies bedeutet, dass einige der verwalteten mobilen Geräte keine PUSH-Benachrichtigungen empfangen. Studieren Sie den HTTP-Code in den Details der Ereignisbeschreibung und reagieren Sie entsprechend. Weitere Informationen über HTTP-Codes, die vom FCM-Server empfangen wurden, und damit verbundene Fehler, entnehmen Sie bitte der Dokumentation von Google Firebase Service (siehe Kapitel "Antwortcodes für nachgeschaltete Nachrichtenfehler").	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Häufige Ereignisse wurde erkannt		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Ereignisse dieser Art treten auf, wenn der Administrationsserver ein häufiges auftretendes Ereignis auf einem verwalteten Gerät erkennt. Weitere Informationen finden Sie im folgenden Abschnitt: Blockieren von häufigen auftretenden Ereignissen.	90 Tage
Die Festplatte ist fast voll	4105	KLSRV_NO_SPACE_ON_VOLUMES	Ereignisse dieser Art treten auf, wenn auf dem Gerät, auf dem der Administrationsserver installiert ist, der Speicherplatz knapp wird. Schaffen Sie freien Speicherplatz.	90 Tage
HTTP-Fehler beim Versenden der FCM-Nachricht an den FCM-Server	4139	KLSRV_GCM_HTTP_ERROR	Ereignisse dieser Art treten auf, wenn die Funktion "Verwaltung mobiler Geräte" so konfiguriert ist, dass sie Google Firebase Cloud Messaging (FCM) für die Verbindung verwalteter Geräte mit Android-Betriebssystem verwendet, und der FCM-Server auf eine Administrationsserver-Anfrage einen anderen HTTP-Code als 200 ("OK") zurück zurückgibt. Im Folgenden werden die Ursachen für das Ereignis und angebrachte Reaktionen darauf ausgeführt: • Probleme mit dem FCM-Server. Studieren Sie den HTTP-Code in den Details der Ereignisbeschreibung und reagieren Sie entsprechend. Weitere Informationen über HTTP-Codes, die vom FCM-Server empfangen wurden, und damit verbundene Fehler, entnehmen Sie bitte der Dokumentation von Google Firebase Service (siehe Kapitel "Antwortcodes für nachgeschaltete Nachrichtenfehler"). • Probleme mit dem Proxyserver (wenn Sie einen Proxyserver benutzen). Studieren Sie den HTTP-Code in den Details des Ereignisses und reagieren Sie entsprechend.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Lizenzbeschränkung wurde überschritten	4098	KLSRV_EV_LICENSE_CHECK_100_110	Kaspersky Security Center Linux überprüft einmal täglich, ob eine Lizenzbeschränkung überschritten wurde. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Beschränkungen der Lizenz durch Kaspersky-Anwendungen, die auf den Client-Geräten installiert sind, überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinheiten die von einer Lizenz abgedeckten werden, 100% bis 110% der von der Lizenz abgedeckten Gesamtzahl an Einheiten überschreitet. Auch wenn dieses Ereignis eintritt, werden die Client-Geräte geschützt. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie ungenutzte Geräte. • Stellen Sie eine Lizenz für weitere Geräte zur Verfügung (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). Kaspersky Security Center Linux ermittelt die Regeln zum Auslösen von Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.	90 Tage
Für eine der lizenzierten Programmgruppen wird die Beschränkung für die Anzahl von Installationen bald erreicht	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Ereignisse dieser Art treten auf, wenn einer der Lizenzschlüssel für Drittanbieter-Programme, die sich in einer lizenzierten Programmgruppe befinden, demnächst abläuft. Dadurch wird für eine der Gruppen die Beschränkung der Anzahl von Installationen reduziert. Sie können auf dieses Ereignis folgendermaßen reagieren: • Wenn die Drittanbieter-Anwendung auf einigen verwalteten Geräten nicht verwendet wird, löschen Sie die Anwendung von diesen Geräten. • Wenn Sie erwarten, dass die Anzahl der Installationen der Drittanbieter-Anwendung das Maximum in nächster Zukunft übersteigt, sollten Sie im Vorfeld den Erwerb einer Drittanbieter-Lizenz für eine größere Anzahl an Geräten in Erwägung ziehen. Sie können die Lizenzschlüssel von Drittanbieteranwendungen verwalten, indem Sie die Funktionen der lizenzierten Anwendungsgruppe verwenden.	90 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Neue Modul-Updates für Kaspersky-Anwendungen wurden registriert	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Ereignisse dieser Art treten auf, wenn der Administrationsserver für Kaspersky-Software, die auf verwalteten Geräten installiert ist, neue Updates registriert, welche eine Genehmigung für die Installation benötigen. Sie können diese Updates in der Kaspersky Security Center Web Console genehmigen oder ablehnen.	90 Tage
Kein freier Platz in der Administrationsserver-Datenbank	4106	KLSRV_NO_SPACE_IN_DATABASE	Ereignisse dieser Art treten auf, wenn der Platz in der Administrationsserver-Datenbank zu knapp ist. Wenn Sie diese Situation nicht lösen, erreicht die Administrationsserver-Datenbank bald ihre Kapazitätsgrenze und der Administrationsserver wird nicht länger funktionieren. Nachfolgend finden Sie die Ursachen für dieses Ereignis in Abhängigkeit vom DBMS, das Sie verwenden, sowie geeignete Reaktionen auf dieses Ereignis. • Begrenzen Sie nicht die Anzahl der Ereignisse, die in der Administrationsserver-Datenbank gespeichert werden sollen. • Reduzieren Sie die Liste an Ereignissen, die in der Administrationsserver-Datenbank gespeichert werden sollen. Überprüfen Sie die Informationen zur Auswahl des DBMS.	90 Tage
Die Maximalanzahl an Ereignissen in der Datenbank wurde überschritten. Es wurde mit dem Löschen von Ereignissen begonnen	4145	KLSRV_EVP_DB_TRUNCATING	Ereignisse dieser Art treten auf, wenn das Löschen älterer Ereignisse aus der Administrationsserver-Datenbank begonnen hat, nachdem die Kapazitätsgrenze der Administrationsserver-Datenbank erreicht wurde. Sie können auf dieses Ereignis folgendermaßen reagieren: • Ändern Sie die maximale Anzahl von Ereignissen, die in der Administrationsserver-Datenbank gespeichert sind. • Reduzieren Sie die Liste an Ereignissen, die in der Datenbank des Administrationsservers gespeichert werden sollen.	Wird nicht gespeichert

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die Maximalanzahl an Ereignissen in der Datenbank wurde überschritten. Die Ereignisse wurden gelöscht	4146	KLSRV_EVP_DB_TRUNCATED	Ereignisse dieser Art treten auf, wenn ältere Ereignisse aus der Administrationsserver-Datenbank gelöscht wurden, nachdem die Kapazitätsgrenze der Administrationsserver-Datenbank erreicht wurde. Sie können auf dieses Ereignis folgendermaßen reagieren: • Ändern Sie die zulässige maximale Anzahl von Ereignissen, die in der Administrationsserver-Datenbank gespeichert sind. • Reduzieren Sie die Liste an Ereignissen, die in der Datenbank des Administrationsservers gespeichert werden sollen.	Wird nicht gespeichert

Ereignisse des Administrationsservers: Information

Die folgende Tabelle enthält die Ereignisse des Kaspersky Security Center Administrationsservers mit der Ereigniskategorie **Information**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** die Einstellungen zur Benachrichtigung und zum Speichern angeben. Für den Administrationsserver können Sie zusätzlich die Ereignisliste in den Eigenschaften des Administrationsservers anzeigen und konfigurieren. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsservers: Information

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Das Zertifikat des Administrationsservers für mobile Geräte wird erneuert	6127	KLSRV_EV_SRV_CERT_RENEWED	Dieses Ereignis tritt auf, wenn das Zertifikat des Administrationsservers erneuert wurde.	30 Tage
Audit: Befehl wurde an Gerät gesendet	4170	KLAUD_EV_COMMAND_SENT	Ereignisse dieses Typs treten auf, wenn der Benutzer einen Befehl an ein mobiles Gerät sendet.	30 Tage
Audit: Die Verbindung mit dem Administrationsserver wurde unterbrochen	4151	KLAUD_EV_SERVERDISCONNECT		30 Tage
Audit: Verbindung mit dem Administrationsserver wurde hergestellt	4147	KLAUD_EV_SERVERCONNECT	Ereignisse dieser Art treten auf, wenn ein Benutzer über die Kaspersky Security Center Web Console eine Verbindung zum Administrationsserver herstellt. Diese Ereignisse enthalten die IP-Adresse des Geräts mit dem installierten Server der Kaspersky Security Center Web Console Server.	30 Tage
Audit: Chiffrierschlüssel importiert/exportiert	5100	KLAUD_EV_DPEKEYSEXPORT	Dieses Ereignis tritt beispielsweise während der Migration auf.	30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Audit: Gruppeneinstellungen modifiziert	4149	KLAUD_EV_ADMGROUP_CHANGED	Ereignisse dieser Art treten auf, wenn eine Sicherheitsgruppe bearbeitet wurde.	30 Tage
Audit: Objekt wurde geändert	4148	KLAUD_EV_OBJECTMODIFY	Dieses Ereignis verfolgt Änderungen in den folgenden Objekten: • Administrationsgruppe • Sicherheitsgruppe • Benutzer • Paket • Aufgabe • Richtlinie • Server • Virtueller Server	30 Tage
Audit: Objekteigenschaften wurden geändert	4152	KLAUD_EV_OBJECTPROPMODIFIED	Dieses Ereignis verfolgt Änderungen der folgenden Eigenschaften: • Benutzer • Lizenz • Server • Virtueller Server	30 Tage
Audit: Objektstatus geändert	4150	KLAUD_EV_TASK_STATE_CHANGED	Dieses Ereignis tritt beispielsweise auf, wenn eine Aufgabe mit einem Fehler beendet wurde.	30 Tage
Audit: testweise Verbindung zu SIEM-Server erfolgreich	5110	KLAUD_EV_SIEM_TEST_SUCCESS	Dieses Ereignis tritt auf, wenn eine testweise Verbindung mit dem SIEM-Server erfolgreich war.	30 Tage
Audit: Benutzerberechtigungen wurden geändert	4153	KLAUD_EV_OBJECTACLMODIFIED	Dieses Ereignis tritt auf, wenn Benutzerberechtigungen geändert wurden.	30 Tage
Die Verbindung mit dem primären Administrationsserver wurde hergestellt	4117	KLSRV_EV_MASTER_SRV_CONNECTED		30 Tage
Die Verbindung mit dem sekundären Administrationsserver wurde hergestellt	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Weitere Informationen dazu finden Sie in folgendem Artikel: Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen.	30 Tage
Datenbanken wurden aktualisiert	4144	KLSRV_UPD_BASES_UPDATED	Ereignisse dieser Art treten ein, wenn die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers** das Aktualisieren der Datenbanken abgeschlossen hat.	30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Gerät wurde automatisch zur Gruppe hinzugefügt	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	Ereignisse dieser Art treten auf, wenn Geräte gemäß den Regeln für das Verschieben von Geräten einer Gruppe zugewiesen wurden.	30 Tage
Das Gerät wurde entsprechend einer Regel automatisch verschoben	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	Ereignisse dieser Art treten auf, wenn Geräte unter Verwendung von Regeln für das Verschieben von Geräten in Administrationsgruppen verschoben wurden.	30 Tage
Das Gerät wurde aus der Gruppe gelöscht: Lange Zeit im Netzwerk inaktiv	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	Ereignisse dieser Art treten auf, wenn Geräte aufgrund von Inaktivität automatisch aus einer Gruppe entfernt wurden.	30 Tage
Die FCM Instance ID hat sich auf diesem mobilen Gerät geändert	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	Ereignisse dieser Art treten auf, wenn sich der Token von Firebase Cloud Messaging auf dem Gerät geändert hat. Informationen zur Rotation des FCM-Tokens finden Sie in der Dokumentation des Firebase-Dienstes.	30 Tage
Datei vom Administrationsserver gelöscht	4163	KLSRV_FILE_REMOVED	Dieses Ereignis tritt auf, wenn eine Datei auf dem Administrationsserver gelöscht wurde.	30 Tage
Datei wurde auf Gerät heruntergeladen	4164	KLSRV_FILE_DOWNLOADED	Dieses Ereignis tritt in den folgenden Fällen auf: • Während einer Sitzung wurde eine Datei auf ein Gerät heruntergeladen. • Eine Datei wurde vom Administrationsserver auf das Gerät heruntergeladen.	30 Tage
Es wurden Dateien gefunden, die zur Analyse an Kaspersky gesendet werden	4131	KLSRV_APS_FILE_APPEARED		30 Tage
Datei auf den Administrationsserver hochgeladen	4162	KLSRV_FILE_UPLOADED	Dieses Ereignis tritt auf, wenn eine Datei auf den Administrationsserver hochgeladen wurde.	30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die Beschränkung für die Anzahl von Installationen wird für eine der lizenzierten Programmgruppen bald überschritten (mehr als 90% verbraucht)	4127	KLSRV_INVLICPROD_FILLED	Ereignisse dieser Art treten auf, wenn die Anzahl der Installationen von Drittanbieter-Anwendungen, die in einer lizenzierten Anwendungsgruppe enthalten sein dürfen, 90% des in den Eigenschaften des Lizenzschlüssels angegeben zulässigen Werts erreicht. Sie können auf dieses Ereignis folgendermaßen reagieren: • Wenn die Drittanbieter-Anwendung auf einigen verwalteten Geräten nicht verwendet wird, löschen Sie die Anwendung von diesen Geräten. • Wenn Sie erwarten, dass die Anzahl der Installationen der Drittanbieter-Anwendung das Maximum in nächster Zukunft übersteigt, sollten Sie im Vorfeld den Erwerb einer Drittanbieter-Lizenz für eine größere Anzahl an Geräten in Erwägung ziehen. Sie können die Lizenzschlüssel von Drittanbieter-Programmen verwalten, indem Sie die Funktionen der lizenzierten Programmgruppe verwenden.	30 Tage
Neues Gerät wurde erkannt	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	Ereignisse dieser Art treten auf, wenn im Netzwerk neue Geräte entdeckt wurden.	30 Tage
Der Lizenzschlüssel ist zu über 90% verbraucht	4097	KLSRV_EV_LICENSE_CHECK_90	Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass einige Lizenzbeschränkungen von auf den Geräten installierten Kaspersky-Anwendungen fast überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinheiten die von einer Lizenz abgedeckten werden, mehr als 90% der von der Lizenz abgedeckten Gesamtzahl an Einheiten überschreitet. Die Client-Geräte sind selbst dann geschützt, wenn eine Lizenzbeschränkung überschritten wird. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie ungenutzte Geräte. • Stellen Sie eine Lizenz für weitere Geräte zur Verfügung (fügen Sie dem Administrationsserver einen gültigen Aktivierungscode oder eine Schlüsseldatei hinzu). Kaspersky Security Center Linux ermittelt die Regeln zum Auslösen von Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.	30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Das Reserve-Zertifikat des Administrationsservers für mobile Geräte wurde erstellt	6126	KLSRV_EV_SRV_CERT_RESERVE_CREATED	Dieses Ereignis tritt auf, wenn das Zertifikat des Administrationsservers erstellt wurde.	30 Tage
Updates wurden erfolgreich in den angegebenen Ordner kopiert	4122	KLSRV_UPD_REPL_OK	Ereignisse dieser Art treten ein, wenn die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsservers** das Kopieren der Dateien in den angegebenen Ordner abgeschlossen hat.	30 Tage

Die Ereignisse **Reservezertifikat wurde erstellt** und **Zertifikat wird erneuert** werden nur dann automatisch vom Administrationsserver veröffentlicht und in der Verwaltungskonsole angezeigt, wenn die Vorgänge, die diesen Ereignissen entsprechen, für die Zertifikate des Administrationsservers für mobile Geräte und UEFI-Geräte ausgeführt werden.

Ereignisse des Administrationsagenten

Dieser Abschnitt informiert über die Ereignisse, die sich auf den Administrationsagenten beziehen.

Ereignisse des Administrationsagenten: Funktionsfehler

Die nachfolgende Tabelle enthält die Ereignisse des Kaspersky Security Center Linux Administrationsagenten mit der Signifikanz **Funktionsfehler**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig konfigurieren möchten, können Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers konfigurieren.

Ereignisse des Administrationsagenten: Funktionsfehler

Angezeigter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die Installation der Root-Zertifikate ist fehlgeschlagen	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	Das Ereignis enthält die Beschreibung des Fehlers, der bei der Installation von Zertifikaten aufgetreten ist.	30 Tage
Installation des Updates für Drittherstellersoftware fehlgeschlagen	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn das Schwachstellen- und Patch-Management verwendet wird und wenn ein Update für Drittanbieter-Programme nicht erfolgreich war. Überprüfen Sie, ob der Link zum Drittanbieter-Programm gültig ist. Lesen Sie die Ereignisbeschreibung.	30 Tage

Angezeigter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Installation der Windows-Updates fehlgeschlagen	7717	KLNAG_EV_WUA_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn Windows-Updates nicht erfolgreich waren. Lesen Sie die Ereignisbeschreibung. Suchen Sie in der Microsoft Knowledge Base nach dem Fehler. Wenden Sie sich an den technischen Support von Microsoft, wenn Sie das Problem nicht selbst lösen können.	30 Tage
Die Root-Zertifikate konnten nicht gelöscht werden	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	Das Ereignis enthält die Beschreibung des Fehlers, der beim Entfernen von Zertifikaten aufgetreten ist.	30 Tage
Das Zurücksetzen der sudoers-Datei auf den Referenzwert ist fehlgeschlagen	7726	KLNAG_EV_SUDOER_RESTORED_ERR	Das Ereignis enthält die Beschreibung des Fehlers, der beim Ersetzen der sudoers-Datei aufgetreten ist.	30 Tage
Fehler bei der Update-Installation	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn das automatische Update und Patchen von Komponenten von Kaspersky Security Center Linux fehlgeschlagen sind. Das Ereignis betrifft nicht die Updates von verwalteten Kaspersky-Anwendungen. Lesen Sie die Ereignisbeschreibung. Ein möglicher Grund für dieses Ereignis ist ein Windows-Problem auf dem Administrationsserver. Wenn die Beschreibung ein Problem in der Windows-Konfiguration erwähnt, beheben Sie dieses Problem.	30 Tage
Benutzerverwaltung: Fehler	7723	KLNAG_EV_USR_MNG_ERR	Ereignis bei einer allgemeinen Warnung.	30 Tage

Ereignisse des Administrationsagenten: Warnung

Die nachfolgende Tabelle enthält die Ereignisse des Administrationsagenten mit der Signifikanz **Warnung**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsagenten: Warnung

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
KSN-Proxy wurde gestartet. Überprüfen der KSN-Verfügbarkeit nicht ausgeführt	7718	KSNPROXY_STARTED_CON_CHK_FAILED	Ereignisse dieser Art treten auf, wenn der Verbindungstest für die konfigurierte Verbindung zum KSN-Proxy fehlschlägt.	30 Tage
Es ist ein Sicherheitsproblem aufgetreten	549	GNRL_EV_APP_INCIDENT_OCCURED	Ereignisse dieser Art treten auf, wenn auf einem Gerät ein Vorfall erkannt wurde. Dieses Ereignis tritt beispielsweise auf, wenn auf dem Gerät nur noch wenig Speicherplatz verfügbar ist.	30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung	Standard-Speicherdauer
Die gefundene sudoers-Datei entspricht nicht dem Referenzwert	7724	KLNAG_EV_SUDOER_DIFFERENT	Ereignisse dieser Art treten auf, wenn die sudoers-Datei nicht mit der Referenzdatei übereinstimmt.	30 Tage
Installation des Updates für Drittherstellersoftware wurde aufgeschoben	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Ereignisse dieser Art treten beispielsweise auf, wenn die EULA für die Installation eines Drittanbieter-Updates abgelehnt wurde.	30 Tage
Installation des Updates für die Drittherstellersoftware wurde mit einer Warnung abgeschlossen	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Laden Sie die Protokolldatei herunter und überprüfen Sie den Wert des Felds KLRI_PATCH_RES_DESC auf Details.	30 Tage
Benutzerverwaltung: Warnungen	7722	KLNAG_EV_USR_MNG_WRN	Ereignis bei einer allgemeinen Warnung.	30 Tage
Während der Installation des Updates des Software-Moduls wurde eine Warnung zurückgegeben	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Laden Sie die Protokolldatei herunter und überprüfen Sie den Wert des Felds KLRI_PATCH_RES_DESC auf Details.	30 Tage

Ereignisse des Administrationsagenten: Information

Die nachfolgende Tabelle enthält die Ereignisse des Administrationsagenten mit der Signifikanz **Information**.

Für jedes Ereignis, das von einem Programm generiert werden kann, können Sie in der Programmrichtlinie auf der Registerkarte **Konfiguration von Ereignissen** Benachrichtigungseinstellungen und Speichereinstellungen festlegen. Wenn Sie die Benachrichtigungseinstellungen für alle Ereignisse gleichzeitig anpassen möchten, konfigurieren Sie die allgemeinen Benachrichtigungseinstellungen in den Eigenschaften des Administrationsservers an.

Ereignisse des Administrationsagenten: Information

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
Anwendung wurde installiert	7703	KLNAG_EV_INV_APP_INSTALLED	30 Tage
Anwendung wurde deinstalliert	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 Tage
Zertifikat des HTTPS-Ports des Webservers wurde abgerufen	—	WEB_SERVER_CERTIFICATE_RENEWED	30 Tage
Gerät wurde autorisiert	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 Tage
Neues Gerät wurde erkannt	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 Tage
Gerät wurde entfernt	7709	KLNAG_EV_DEVICE_REMOVE	30 Tage
Installation des Updates des Software-Moduls wurde gestartet	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 Tage
KSN-Proxy wurde gestartet. Überprüfung der KSN-Verfügbarkeit wurde erfolgreich abgeschlossen	7719	KSNPROXY_STARTED_CON_CHK_OK	30 Tage
KSN-Proxy wurde angehalten	7720	KSNPROXY_STOPPED	30 Tage
Überwachte Anwendung wurde installiert	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 Tage
Überwachte Anwendung wurde deinstalliert	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 Tage
Neues Gerät wurde hinzugefügt	7708	KLNAG_EV_DEVICE_ARRIVAL	30 Tage
Root-Zertifikate wurden installiert	7727	KLNAG_EV_ROOT_CERT_INSTALLED	30 Tage
Root-Zertifikate wurden entfernt	7729	KLNAG_EV_ROOT_CERT_REMOVED	30 Tage

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Standard-Speicherdauer
Sudoers-Datei wurde erfolgreich auf Referenzwert zurückgesetzt	7725	KLNAG_EV_SUDOER_RESTORED	30 Tage
Drittherstelleranwendung wurde installiert	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 Tage
Update für Drittherstellersoftware wurde erfolgreich installiert	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 Tage
Installation des Updates von Drittherstellersoftware wurde gestartet	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 Tage
Update für Software-Module wurde erfolgreich installiert	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 Tage
Benutzerverwaltung: Informationen	7721	KLNAG_EV_USR_MNG_INF	30 Tage
Webserver wurde auf dem Host gestartet	—	WEB_SERVER_STARTED	30 Tage
Webserver wurde auf dem Host gestoppt	—	WEB_SERVER_STOPPED	30 Tage
Windows Desktopfreigabe: Die Anwendung wurde gestartet	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 Tage
Windows Desktopfreigabe: Datei wurde geändert	7713	KLUSRLOG_EV_FILE_MODIFIED	30 Tage
Windows Desktopfreigabe: Datei wurde gelesen	7712	KLUSRLOG_EV_FILE_READ	30 Tage
Windows Desktopfreigabe: Gestartet	7715	KLUSRLOG_EV_WDS_BEGIN	30 Tage
Windows Desktopfreigabe: Beendet	7716	KLUSRLOG_EV_WDS_END	30 Tage

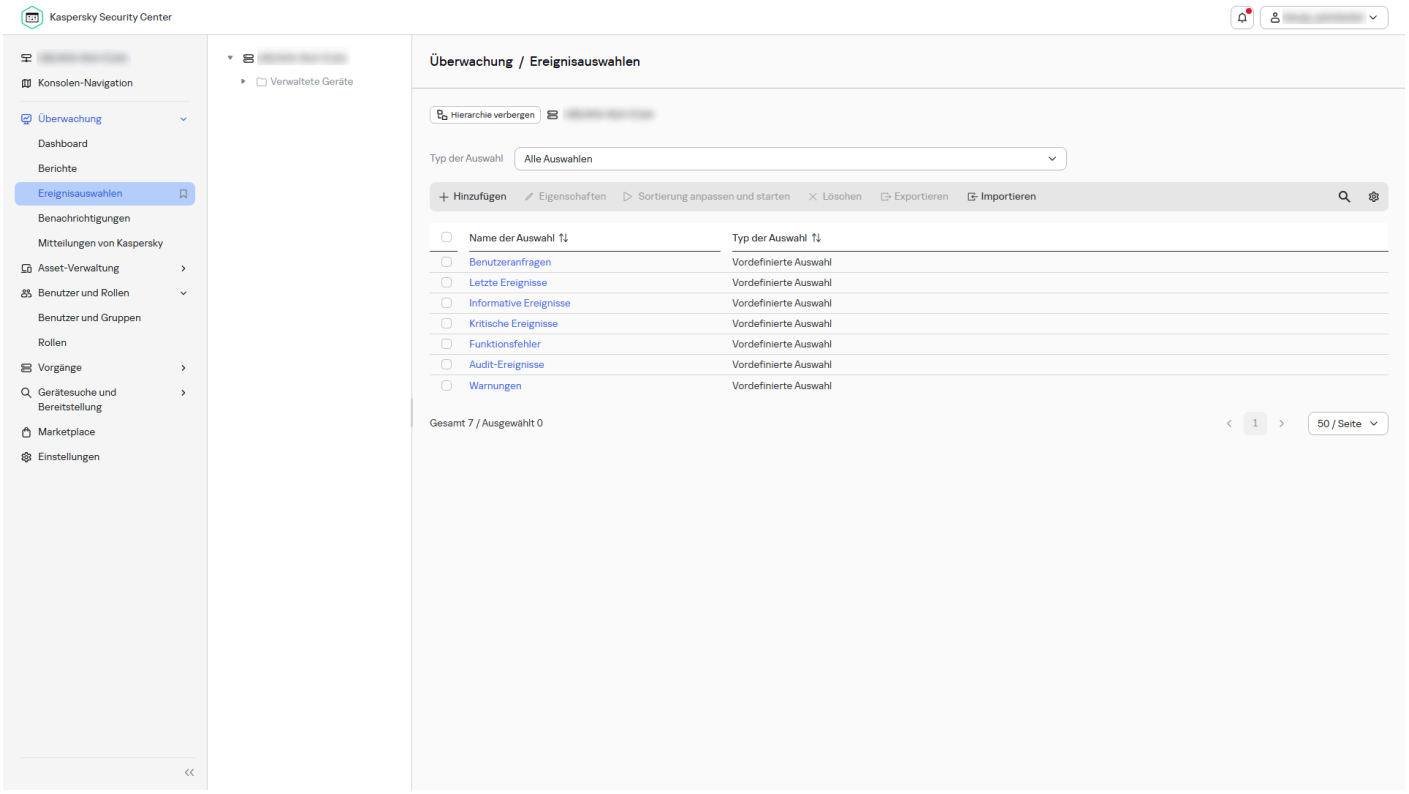
Ereignisauswahlen verwenden

Die Ereignisauswahlen bieten eine Bildschirmansicht der benannten Ereignisgruppen, die aus der Administrationsserver-Datenbank ausgewählt wurden. Diese Sätze von Ereignissen sind nach den folgenden Kategorien gruppiert:

- Nach Ereigniskategorie – **Kritische Ereignisse**, **Funktionsfehler**, **Warnungen** und **Informative Ereignisse**
- Nach Zeit – **Letzte Ereignisse**
- Nach Typ – **Benutzeranfragen** und **Audit-Ereignisse**

Benutzerdefinierte Ereignisauswahlen können Sie auf der Basis von Einstellungen, die in der Oberfläche von Kaspersky Security Center Web Console verfügbar sind, erstellen und anzeigen.

Ereignisauswahlen finden Sie in Kaspersky Security Center Web Console im Abschnitt **Überwachung** unter **Ereignisauswahlen**.



Die Liste der Ereignisauswahlen

Standardmäßig enthalten Ereignisauswahlen Informationen für die letzten sieben Tage.

Kaspersky Security Center Linux besitzt eine Standardauswahl von (vordefinierten) Ereignisauswahlen:

- Ereignisse mit unterschiedlichen Ereigniskategorien:
  - **Kritische Ereignisse**
  - **Funktionsfehler**
  - **Warnungen**
  - **Informative Ereignisse**
- **Benutzeranfragen** (Ereignisse von verwalteten Anwendungen)
- **Letzte Ereignisse** (der letzten Woche)
- Audit-Ereignisse

Sie können auch zusätzliche benutzerdefinierte Auswahlen definieren und anpassen. In benutzerdefinierten Auswahlen können Sie Ereignisse nach den Eigenschaften der Geräte, von denen sie stammen, (Gerätenamen, IP-Bereiche und Administrationsgruppen), nach Ereignistypen und Signifikanzen, nach Anwendung und Komponentenname, sowie nach Zeitraum filtern. Es ist auch möglich, Ergebnisse der Aufgabenausführung in den Suchbereich aufzunehmen. Sie können auch ein einfaches Suchfeld verwenden, in das ein Wort oder mehrere Wörter eingegeben werden können. Alle Ereignisse, die irgendwo in den Attributen (wie Ereignisname, Beschreibung, Komponentenname) eines der eingegebenen Wörter enthalten, werden angezeigt.

Sowohl für vordefinierte als auch benutzerdefinierte Auswahlen können Sie die Zahl der angezeigten Ereignisse oder die Anzahl der Einträge, die gesucht werden sollen, begrenzen. Beide Optionen wirken sich auf die Zeit aus, die Kaspersky Security Center Linux für die Anzeige der Ereignisse benötigt. Je größer die Datenbank ist, desto zeitaufwändiger kann der Prozess sein.

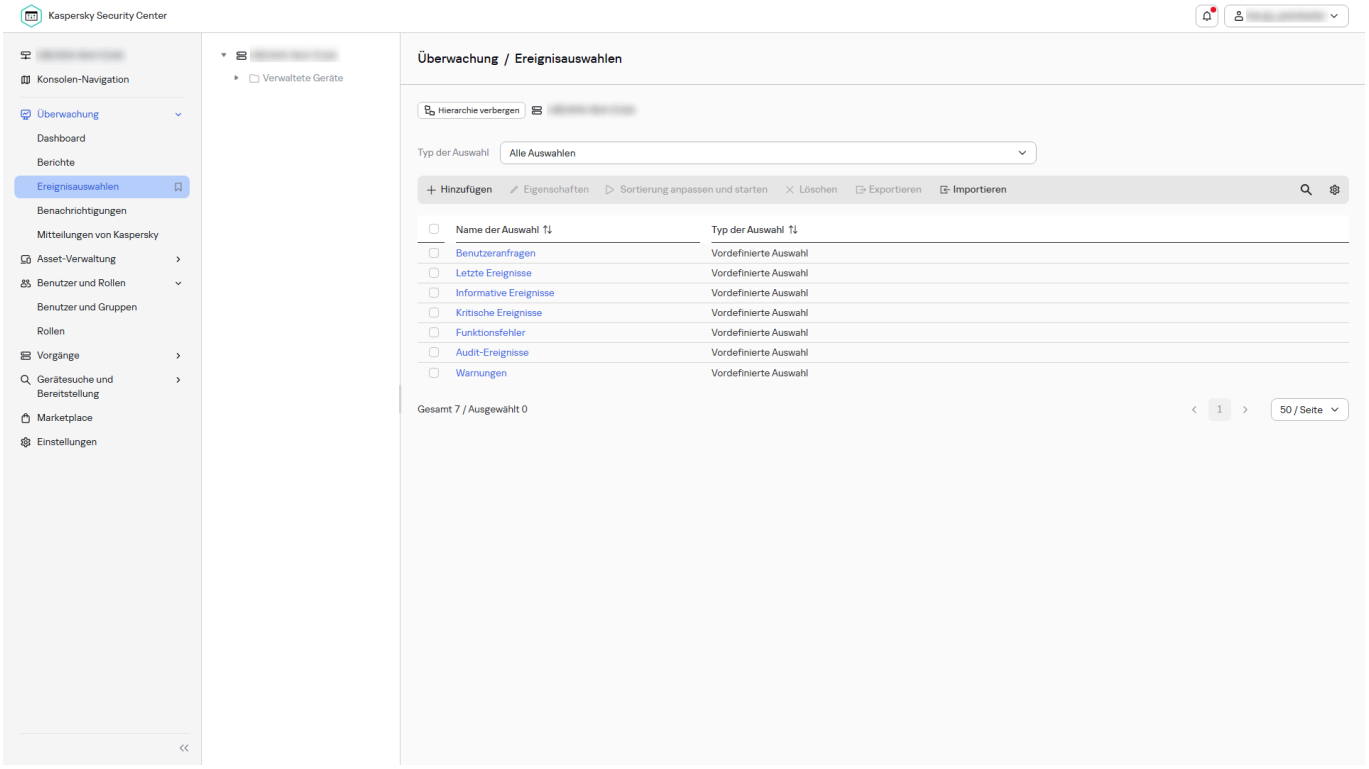
Sie können Folgendes tun:

- Eigenschaften von Ereignisauswahlen bearbeiten
- Ereignisauswahlen erstellen
- Details der Ereignisauswahlen anzeigen
- Ereignisauswahlen löschen
- Ereignisse aus der Administrationsserver-Datenbank löschen

Ereignisauswahl erstellen

Um eine Ereignisauswahl zu erstellen, gehen Sie wie folgt vor:

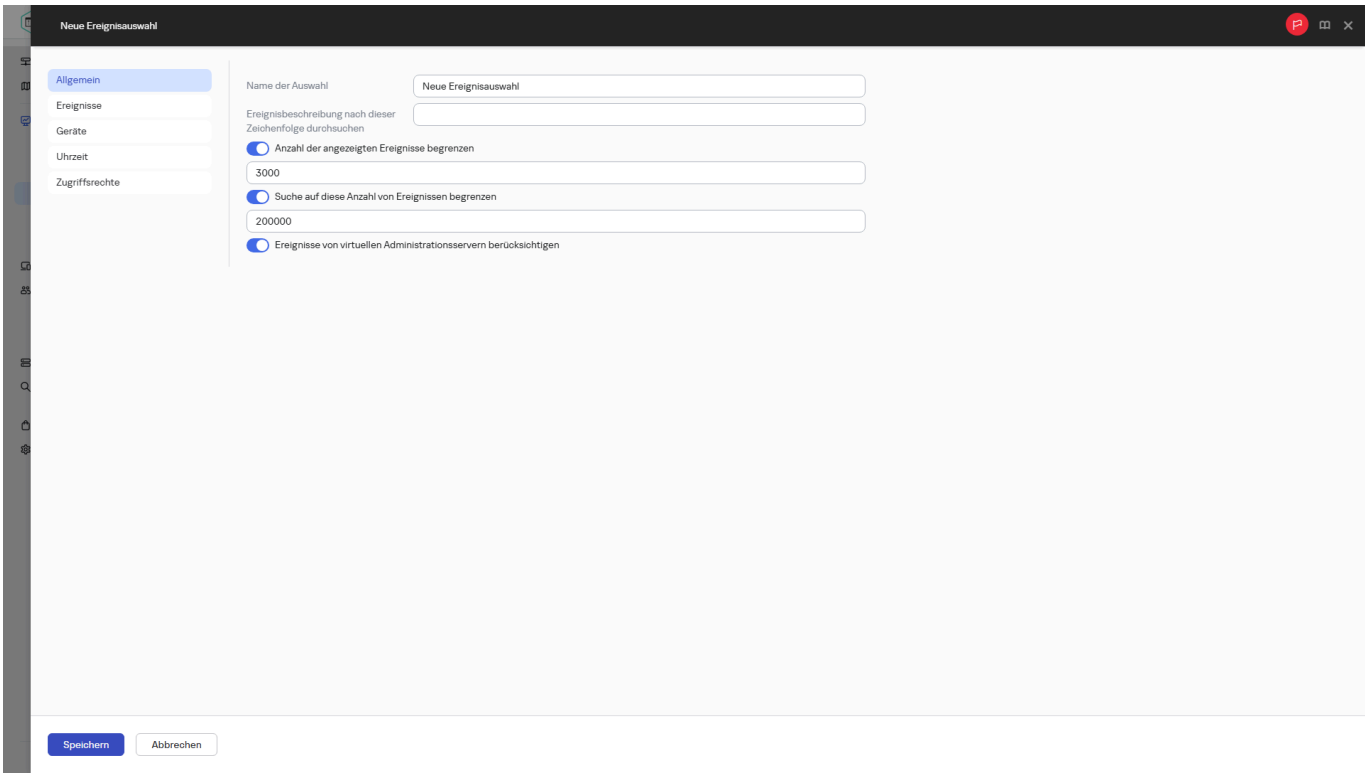
1. Gehen Sie im Hauptmenü zu **Überwachung → Ereignisauswahlen**.



Die Liste der Ereignisauswahlen

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

3. Geben Sie im folgenden Fenster **Neue Ereignisauswahl** die Einstellungen der neuen Ereignisauswahl an. Tun Sie dies in einem oder mehreren der Abschnitte im Fenster.



Erstellen einer neuen Ereignisauswahl

4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

   Das Bestätigungsfenster öffnet sich.

5. Um das Ergebnis der Ereignisauswahl anzuzeigen, lassen Sie das Kontrollkästchen **Zum Ergebnis der Auswahl wechseln** aktiviert.

6. Klicken Sie auf **Speichern**, um die Erstellung der Ereignisauswahl zu bestätigen.

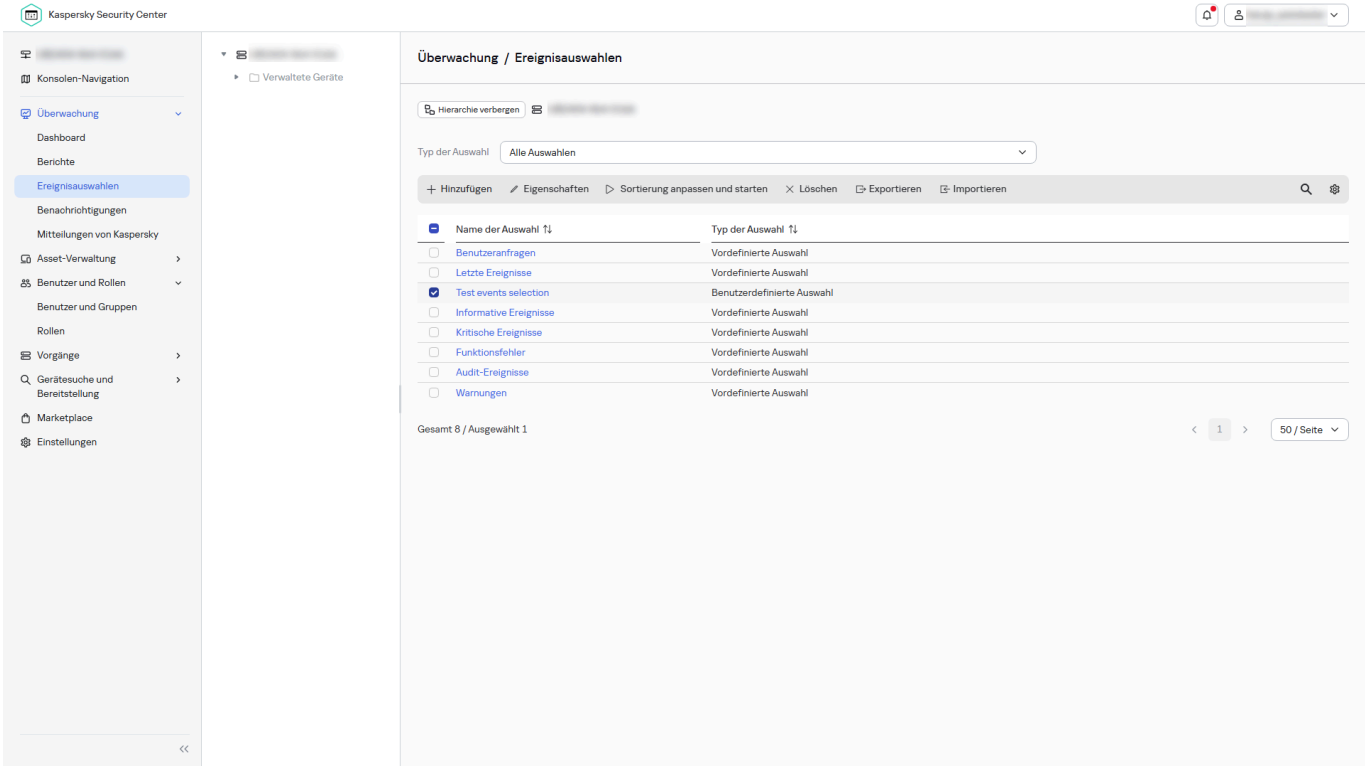
Wenn Sie das Kontrollkästchen **Zum Ergebnis der Auswahl wechseln** aktiviert lassen, wird das Ergebnis der Ereignisauswahl angezeigt. Andernfalls wird die neue Ereignisauswahl in der Liste der Ereignisauswahl angezeigt.

Ereignisauswahl bearbeiten

Um eine Ereignisauswahl zu bearbeiten, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung → Ereignisauswahlen**.

2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie bearbeiten möchten.



Die Liste der Ereignisauswahlen

3. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Ein Fenster mit den Einstellungen der Ereignisauswahl wird geöffnet.

4. Bearbeiten Sie die Eigenschaften der Ereignisauswahl.

   Bei vordefinierten Ereignisauswahlen können Sie nur die Eigenschaften auf den folgenden Registerkarten bearbeiten: **Allgemein** (mit Ausnahme des Namens der Auswahl), **Uhrzeit** und **Zugriffsrechte**.

   Bei benutzerdefinierten Auswahlen können alle Eigenschaften bearbeitet werden.

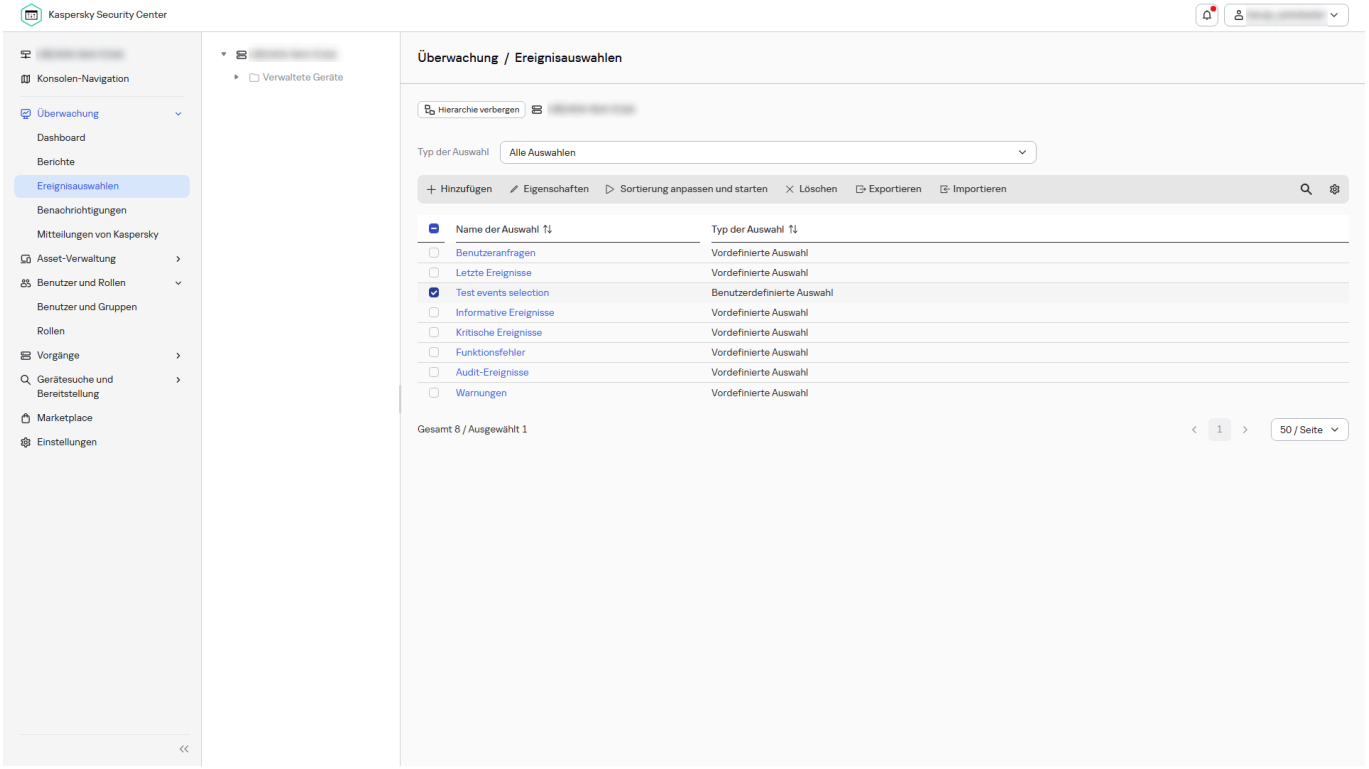
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Die bearbeitete Ereignisauswahl wird in der Liste angezeigt.

Liste mit einer Ereignisauswahl anzeigen

Um eine Ereignisauswahl anzuzeigen:

1. Gehen Sie im Hauptmenü zu **Überwachung** → **Ereignisauswahlen**.
2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie starten möchten.



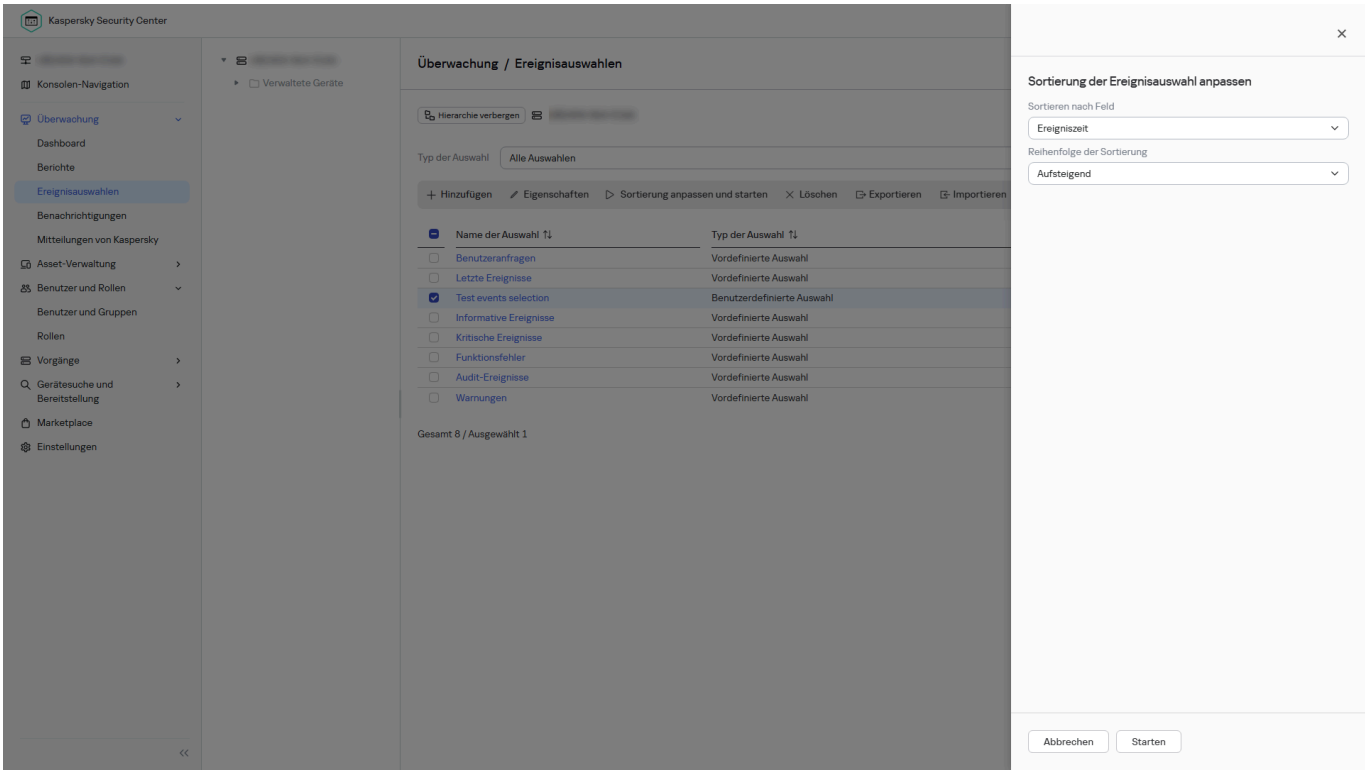
Die Liste der Ereignisauswahlen

3. Führen Sie eine der folgenden Aktionen aus:

- Um die Sortierung der Ergebnisse der Ereignisauswahl anzupassen, gehen Sie wie folgt vor:

  a. Klicken Sie auf die Schaltfläche **Sortierung anpassen und starten**.

  b. Geben Sie im Fenster **Sortierung der Ereignisauswahl anpassen** die Einstellungen für die Sortierung an.

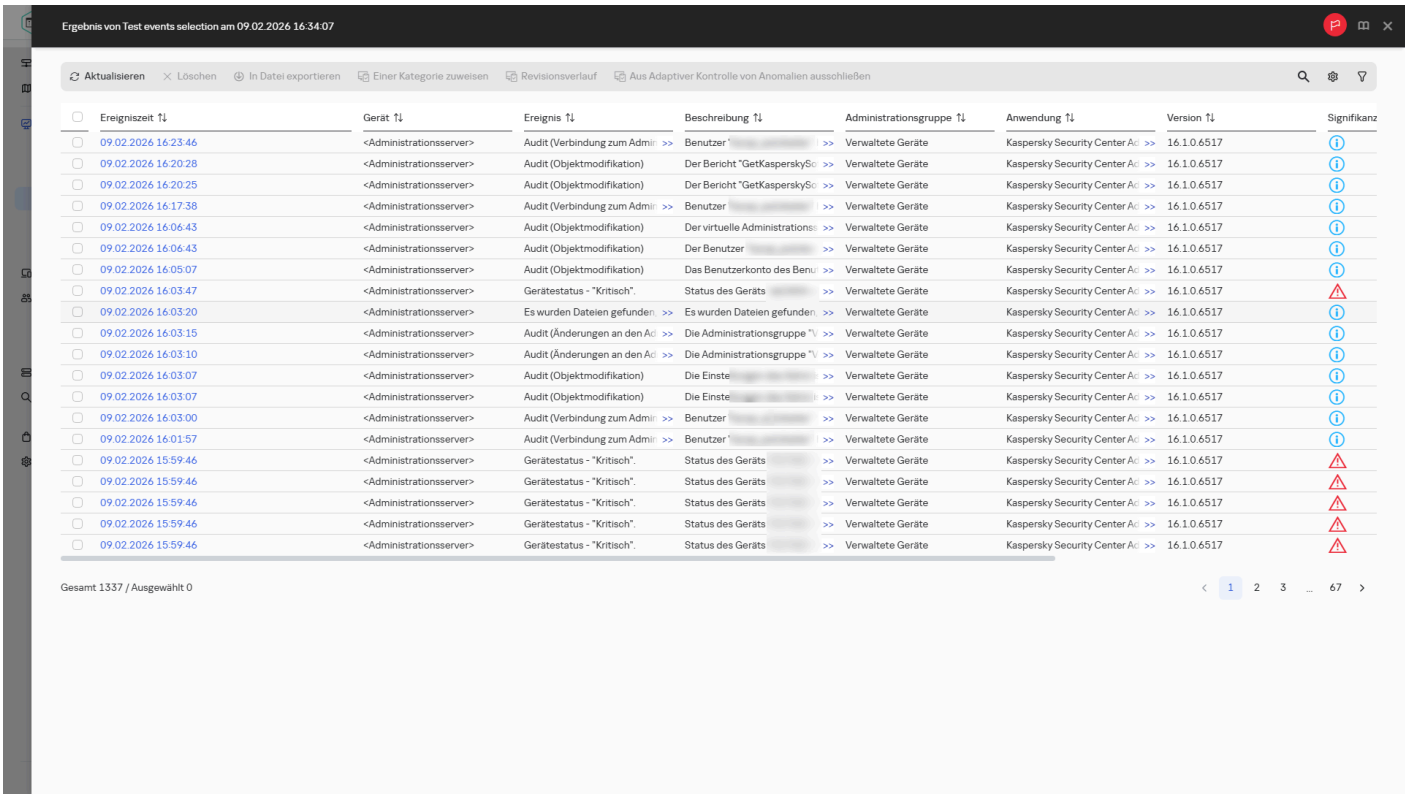


Festlegen der Sortiereinstellungen der Ereignisauswahl

  a. Klicken Sie auf den Namen der Auswahl.

- Um die Liste der Ereignisse so anzuzeigen, wie sie auf dem Administrationsserver sortiert ist, klicken Sie auf den Namen der Auswahl.

Das Ergebnis der Ereignisauswahl wird angezeigt.



Das Ergebnis der Ereignisauswahl

Ereignisauswahl exportieren

Mit Kaspersky Security Center Linux können Sie eine Ereignisauswahl und deren Einstellungen in einer klo-Datei speichern. Sie können diese klo-Datei verwenden, um sowohl in Kaspersky Security Center Windows als auch in Kaspersky Security Center Linux die gespeicherte Ereignisauswahl zu importieren.

Beachten Sie, dass Sie nur benutzerdefinierte Ereignisauswahlen exportieren können. Ereignisauswahlen aus dem Standardumfang von Kaspersky Security Center Linux (vordefinierte Auswahlen) können nicht in einer Datei gespeichert werden.

So exportieren Sie eine Ereignisauswahl:

1. Wechseln Sie im Hauptmenü zu **Überwachung** → **Ereignisauswahlen**.
2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie exportieren möchten.

   Sie können nicht mehrere Ereignisauswahlen gleichzeitig exportieren. Wenn Sie mehr als eine Auswahl auswählen, wird die Schaltfläche **Exportieren** deaktiviert.
3. Klicken Sie auf die Schaltfläche **Exportieren**.
4. Geben Sie im neuen Fenster **Speichern als** den Namen und den Pfad der Datei mit der Ereignisauswahl an und klicken Sie anschließend auf die Schaltfläche **Speichern**.

   Das Fenster **Speichern unter** wird nur angezeigt, wenn Sie Google Chrome, Microsoft Edge oder Opera verwenden. Wenn Sie einen anderen Browser verwenden, wird die Datei mit der Ereignisauswahl automatisch im Ordner **Downloads** gespeichert.

Ereignisauswahl importieren

Mit Kaspersky Security Center Linux können Sie eine Ereignisauswahl aus einer klo-Datei importieren. Die klo-Datei enthält die exportierte Ereignisauswahl und deren Einstellungen.

So importieren Sie eine Ereignisauswahl:

1. Wechseln Sie im Hauptmenü zu **Überwachung** → **Ereignisauswahlen**.
2. Klicken Sie auf die Schaltfläche **Importieren**, um eine Datei mit der Ereignisauswahl auszuwählen, die Sie importieren möchten.
3. Geben Sie im folgenden Fenster den Pfad zur klo-Datei an und klicken Sie anschließend auf die Schaltfläche **Öffnen**. Beachten Sie, dass Sie nur eine Ereignisauswahl-Datei auswählen können.

   Die Verarbeitung der Ereignisauswahl beginnt.

Die Benachrichtigung mit dem Resultat des Imports wird angezeigt. Wenn die Ereignisauswahl erfolgreich importiert wurde, können Sie auf den Link **Importdetails anzeigen** klicken, um die Eigenschaften der Ereignisauswahl anzuzeigen.

Nach einem erfolgreichen Import wird die Ereignisauswahl in der Liste der Auswahlen angezeigt. Die Einstellungen der Ereignisauswahl werden ebenfalls importiert.

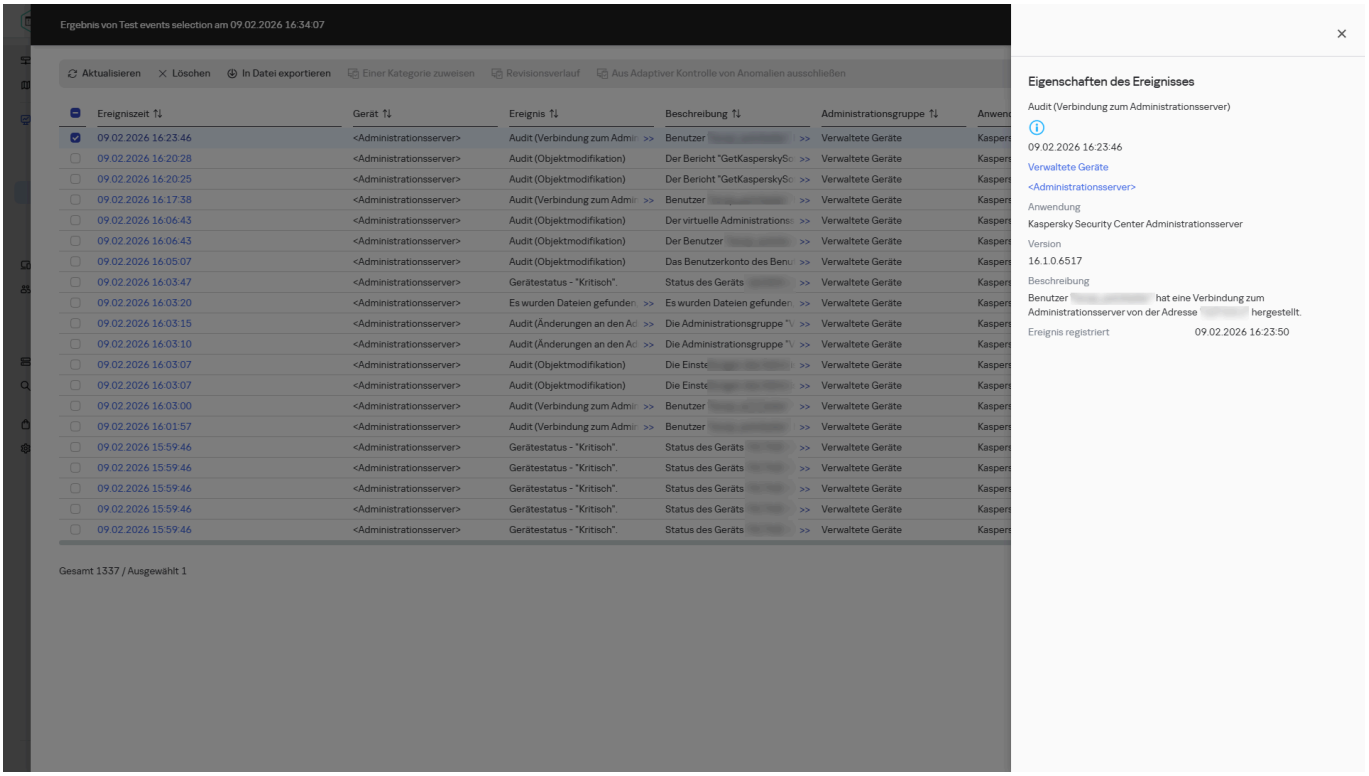
> Wenn die neu importierte Ereignisauswahl denselben Namen wie eine bereits vorhandene Ereignisauswahl besitzt, wird der Name der importierten Auswahl um den Index **(<nächste folgende Nummer>)** erweitert, zum Beispiel: **(1)**, **(2)**.

Informationen zu einem Ereignis anzeigen

So zeigen Sie Informationen zu einem Ereignis an:

1. Starten Sie eine Ereignisauswahl.
2. Klicken Sie auf die Uhrzeit des gewünschten Ereignisses.

Das Fenster **Eigenschaften des Ereignisses** wird geöffnet.



Das Fenster mit den Ereigniseigenschaften

3. Im angezeigten Fenster können Sie Folgendes tun:

   - Informationen zum ausgewählten Ereignis ansehen
   - Zum Gerät wechseln, auf dem das Ereignis eingetreten ist
   - Zur Administrationsgruppe wechseln, die das Gerät enthält, auf dem das Ereignis eingetreten ist
   - Zu den Aufgabeneigenschaften wechseln, wenn sich das Ereignis auf eine Aufgabe bezieht

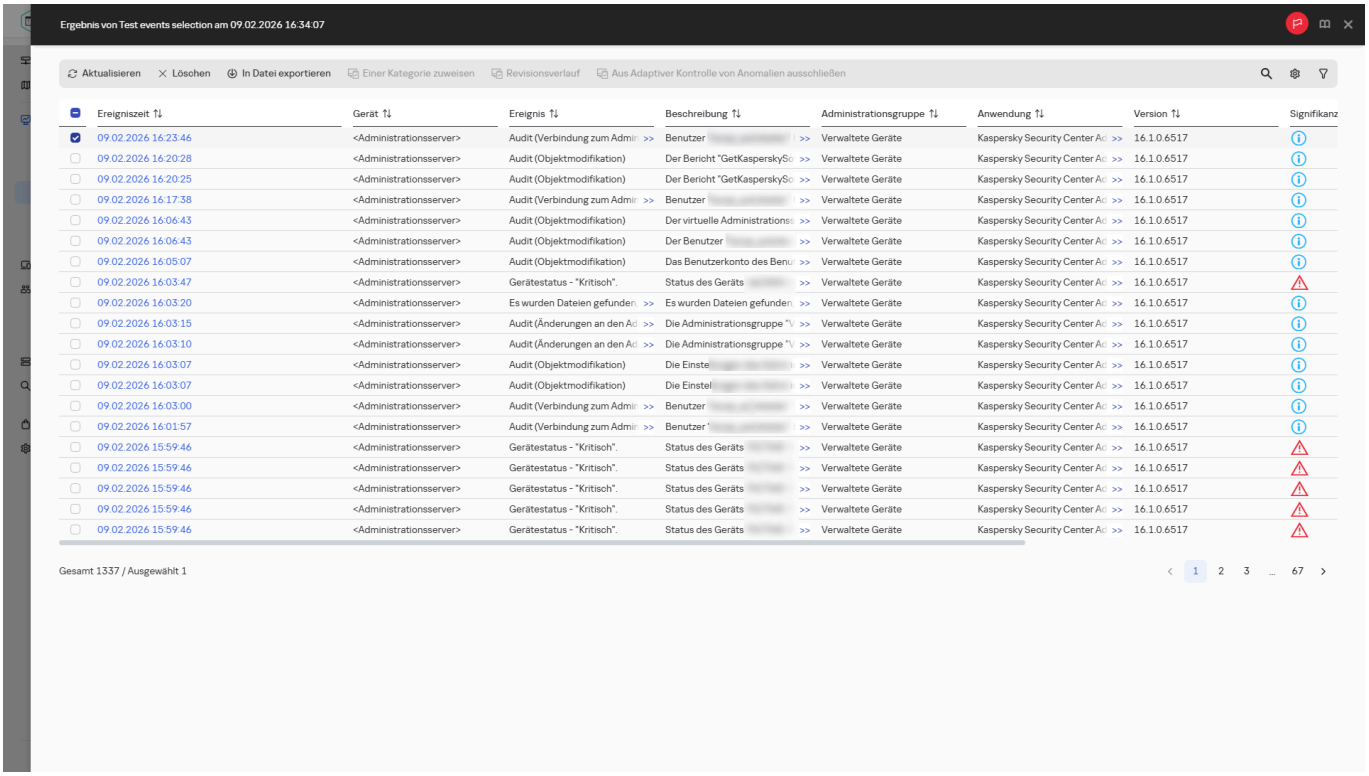
Ereignisse in eine Datei exportieren

Mit Kaspersky Security Center Linux können Sie Ereignisse aus einer Ereignisauswahl in einer txt-Datei speichern.

Um Ereignisse in eine Datei zu exportieren, gehen Sie wie folgt vor:

1. Starten einer Ereignisauswahl.
2. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Ereignis.

Sie können auch mehrere Ereignisse oder die gesamte Ereignisauswahl auswählen.



Das Ergebnis der Ereignisauswahl

3. Klicken Sie auf die Schaltfläche **In Datei exportieren**.

   Das ausgewählte Ereignis wird in eine txt-Datei exportiert.

Verlauf eines Objekts aus einem Ereignis heraus anzeigen

Sie können aus einem Ereignis zur Erstellung oder Änderung eines Objekts, das Revisionsverwaltung unterstützt, zum Revisionsverlauf dieses Objekts wechseln.

Um den Verlauf eines Objekts aus einem Ereignis heraus anzuzeigen, gehen Sie wie folgt vor:

1. Starten einer Ereignisauswahl.
2. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Ereignis.
3. Klicken Sie auf die Schaltfläche **Revisionsverlauf**.

   Der Revisionsverlauf des Objekts wird geöffnet.

Ereignisse löschen

So löschen Sie Ereignisse aus einer Ereignisauswahl:

1. Starten einer Ereignisauswahl.
2. Wählen Sie die Ereignisse aus:
   - Aktivieren Sie die Kontrollkästchen neben allen Ereignissen, die Sie löschen möchten.
   - Wenn Sie alle Ereignisse auf der aktuellen Seite löschen möchten, aktivieren Sie das Kontrollkästchen über der Liste mit den Ereignissen und klicken Sie auf die Option **Alle auf aktueller Seite auswählen**.
   - Wenn Sie alle Ereignisse aus einer Auswahl löschen möchten, aktivieren Sie das Kontrollkästchen über der Liste und klicken Sie auf die Option **Alle auswählen**.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im neuen Fenster auf **Löschen**.

So löschen Sie Ereignisse aus einer Liste mit Geräteereignissen:

1. Öffnen Sie die Geräteliste.
   - Für verwaltete Geräte: **Asset-Verwaltung** → **Assets (Geräte)**.
   - Für nicht zugeordnete Geräte: **Asset-Verwaltung** → **Nicht zugeordnete Geräte**.
2. Klicken Sie in der Geräteliste auf den Link mit dem Namen des gewünschten Geräts und wechseln Sie anschließend zur Registerkarte **Ereignisse**.
3. Wählen Sie die Ereignisse aus:
   - Aktivieren Sie die Kontrollkästchen neben allen Ereignissen, die Sie löschen möchten.
   - Wenn Sie alle Ereignisse auf der aktuellen Seite löschen möchten, aktivieren Sie das Kontrollkästchen über der Liste mit den Ereignissen und klicken Sie auf die Option **Alle auf aktueller Seite auswählen**.
   - Wenn Sie alle Ereignisse aus einer Auswahl löschen möchten, aktivieren Sie das Kontrollkästchen über der Liste und klicken Sie auf die Option **Alle auswählen**.
4. Klicken Sie auf **Löschen** und bestätigen Sie anschließend die Aktion.
5. Klicken Sie im neuen Fenster auf **Löschen**.

Die ausgewählten Ereignisse werden gelöscht und können nicht wiederhergestellt werden.

Ereignisauswahl löschen

Sie können nur benutzerdefinierte Ereignisauswahlen löschen. Vordefinierte Ereignisauswahlen können nicht gelöscht werden.

Um eine oder mehrere Ereignisauswahlen zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung** → **Ereignisauswahlen**.
2. Aktivieren Sie die Kontrollkästchen neben den Ereignisauswahlen, die Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **OK**.

Die Ereignisauswahl ist gelöscht.

Speicherdauer für ein Ereignis festlegen

Kaspersky Security Center Linux ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Kaspersky-Anwendungen aufgetreten sind. Die Informationen über Ereignisse werden in der Administrationsserver-Datenbank gespeichert. Möglicherweise sollen bestimmte Ereignisse länger oder kürzer aufbewahrt werden, als durch die Standardwerte vorgegeben. Sie können die Standardeinstellungen der Speicherdauer für ein Ereignis ändern.

Wenn Sie bestimmte Ereignisse nicht in der Administrationsserver-Datenbank speichern möchten, können Sie die entsprechende Einstellung deaktivieren. Verwenden Sie dazu die Administrationsserver-Richtlinie und die Richtlinie der Kaspersky-Anwendung oder die Administrationsserver-Eigenschaften (nur für Administrationsserver-Ereignisse). Dadurch wird die Anzahl der Ereignistypen in der Datenbank reduziert.

Je länger die Speicherdauer eines Ereignisses, desto schneller erreicht die Datenbank ihre maximale Kapazität. Eine längere Speicherdauer für ein Ereignis ermöglicht es Ihnen aber, Überwachungs- und Berichtsaufgaben über einen längeren Zeitraum durchzuführen.

So legen Sie die Speicherdauer für ein Ereignis in der Administrationsserver-Datenbank fest:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.
2. Klicken Sie auf den Namen der gewünschten Richtlinie.

   Sie können eine Richtlinie für eine verwaltete Kaspersky-Anwendung, den Administrationsagenten oder den Administrationsserver auswählen. Für den Administrationsserver können Sie die Speicherdauer der Ereignisse auch anpassen, indem Sie auf den Namen des Administrationsservers klicken.
3. Wählen Sie die Registerkarte **Konfiguration von Ereignissen** aus.

   Eine Liste der Ereignistypen, die sich auf den Abschnitt **Kritisch** beziehen, wird angezeigt. Bei Bedarf können Sie zu den Abschnitten **Funktionsfehler**, **Warnung** oder **Information** wechseln.

4. Klicken Sie in der Liste der Ereignistypen im rechten Bereich auf den Link für das Ereignis, dessen Speicherdauer Sie ändern möchten.

   Im Abschnitt **Ereignisregistrierung** des sich öffnenden Fensters ist der Umschalter **In der Administrationsserver-Datenbank speichern für (Tage)** aktiviert.

5. Geben Sie im Bearbeitungsfeld unterhalb dieser Umschalttaste die Anzahl der Tage ein, über die das Ereignis gespeichert werden soll.

6. Wenn Sie ein Ereignis nicht in der Administrationsserver-Datenbank speichern möchten, deaktivieren Sie die Option **In der Administrationsserver-Datenbank speichern für (Tage)**.

   > Wenn Sie Administrationsserver-Ereignisse im Eigenschaftenfenster des Administrationsservers anpassen und wenn die Ereigniseinstellungen in der Richtlinie des Kaspersky Security Center Administrationsservers gesperrt sind, können Sie die Speicherdauer für ein Ereignis nicht ändern.

7. Klicken Sie auf **OK** und nach dem Schließen des rechten Bereichs auf die Schaltfläche **Speichern**.

   Das Eigenschaftenfenster der Richtlinie wird geschlossen.

Die Ereignisse des ausgewählten Typs, die vom Administrationsserver empfangen und gespeichert werden, besitzen ab jetzt die geänderte Speicherfrist. Für zuvor empfangene Ereignisse ändert der Administrationsserver die Speicherfrist nicht.

Häufige auftretende Ereignisse blockieren

Dieser Abschnitt enthält Informationen zur Verwaltung des Blockierens häufig auftretender Ereignisse sowie zum Aufheben der Blockade häufig auftretender Ereignisse.

Über das Blockieren von häufig auftretenden Ereignissen

Eine verwaltete Anwendung (z. B. Kaspersky Endpoint Security für Linux), die auf einem oder mehreren verwalteten Geräten installiert ist, sendet möglicherweise viele Ereignisse des gleichen Typs an den Administrationsserver. Das Empfangen häufig auftretender Ereignisse kann die Administrationsserver-Datenbank überlasten und führt zum Überschreiben anderer Ereignisse. Der Administrationsserver beginnt, die am häufigsten auftretenden Ereignisse zu blockieren, wenn die Anzahl aller empfangenen Ereignisse den für die Datenbank festgelegten Grenzwert überschreitet.

> Der Administrationsserver blockiert den Empfang von häufig auftretenden Ereignissen automatisch. Sie können die häufig auftretenden Ereignisse nicht selbst blockieren und auch nicht festlegen, welche Ereignisse blockiert werden sollen.

Um herauszufinden, ob ein Ereignis blockiert wird, können Sie die Liste mit Benachrichtigung anzeigen oder überprüfen, ob das Ereignis im Abschnitt **Blockieren häufiger Ereignisse** des Administrationsservers aufgeführt ist. Wenn das Ereignis blockiert ist, können Sie Folgendes tun:

- Wenn Sie verhindern möchten, dass die Datenbank überschrieben wird, können Sie das Empfangen dieser Ereignistypen weiterhin blockieren.
- Wenn Sie beispielsweise den Grund für das häufige Senden eines Ereignisses an den Administrationsserver ermitteln möchten, können Sie häufig auftretende Ereignisse entsperren und die Ereignisse dieses Typs auf diese Weise weiterhin empfangen.
- Wenn Sie die häufig auftretenden Ereignisse weiterhin so lange empfangen möchten, bis sie wieder blockiert werden, können Sie für die häufig auftretenden Ereignisse die Blockierung entfernen.

Das Blockieren häufig auftretender Ereignissen verwalten

Der Administrationsserver blockiert den automatischen Empfang von häufig auftretenden Ereignissen, aber Sie können die Blockade aufheben und häufig auftretende Ereignisse weiterhin empfangen. Sie können außerdem den Empfang häufig auftretender Ereignisse blockieren, deren Blockade Sie zuvor aufgehoben haben.

Um das Blockieren von häufig auftretenden Ereignissen zu verwalten:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Blockieren häufig auftretender Ereignisse** aus.

3. Im Abschnitt **Blockieren häufig auftretender Ereignisse**:

   - Wenn Sie das Blockieren des Empfangs häufig auftretender Ereignisse aufheben möchten:

     a. Wählen Sie die häufig auftretenden Ereignisse aus, die Sie entsperren möchten, und klicken Sie anschließend auf die Schaltfläche **Ausschließen**.

     b. Klicken Sie auf **Speichern**.

   - Um häufig auftretende Ereignisse zu blockieren:

     a. Wählen Sie die häufig auftretenden Ereignisse aus, die Sie blockieren möchten, und klicken Sie auf **Blockieren**.

     b. Klicken Sie auf **Speichern**.

Der Administrationsserver empfängt die entsperrten häufig auftretenden Ereignisse und empfängt keine blockierten häufig auftretende Ereignisse.

Die Blockade häufig auftretender Ereignisse aufheben

Sie können die Blockade für häufig auftretende Ereignisse aufheben und diese so lange empfangen, bis der Administrationsserver diese häufig auftretenden Ereignissen erneut blockiert.

So heben Sie die Blockade für häufig auftretende Ereignisse auf:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Blockieren häufig auftretender Ereignisse** aus.

3. Wählen Sie im Abschnitt **Blockieren häufig auftretender Ereignisse** die Arten häufig auftretender Ereignisse, für die Sie die Blockade aufheben möchten.

4. Klicken Sie auf **Blockade aufheben**.

Das häufig auftretende Ereignis wird aus der Liste der häufig auftretenden Ereignisse entfernt. Der Administrationsserver empfängt Ereignisse dieses Typs.

Ereignisse auf dem Administrationsserver verarbeiten und speichern

Die Informationen zu Ereignissen, die während der Ausführung der Anwendung und der verwalteten Geräte auftreten, werden in der Administrationsserver-Datenbank gespeichert. Jedes Ereignis gehört einem bestimmten Typ und einer Signifikanz (*Kritisches Ereignis*, *Funktionsfehler*, *Warnung*, *Infomeldung*) an. Abhängig von den Umständen, unter denen das Ereignis aufgetreten ist, können Ereignissen eines Typs von der Anwendung verschiedene Signifikanzen zugeordnet werden.

Die Typen und Signifikanzen können Sie im Eigenschaftenfenster des Administrationsservers im Abschnitt **Ereignisse konfigurieren** anzeigen. Ferner können Sie im Abschnitt **Ereignisse konfigurieren** die Einstellungen für die Verarbeitung der einzelnen Ereignisse durch den Administrationsserver anpassen:

- Ereignisse auf dem Administrationsserver und in den Ereignisprotokollen des Betriebssystems auf dem Gerät und auf dem Administrationsserver erfassen

- Benachrichtigungsmethode des Administrators über die Ereignisse (beispielsweise SMS, E-Mail-Nachricht)

Im Eigenschaftenfenster des Administrationsservers können Sie im Abschnitt **Ereignis-Datenverwaltung** die Einstellungen für das Speichern der Ereignisse in der Administrationsserver-Datenbank anpassen: Anzahl der Einträge über Ereignisse und Speicherdauer der Einträge beschränken. Wenn Sie die maximale Anzahl der Ereignisse angeben, berechnet die Anwendung einen ungefähren Wert des für die angegebene Zahl benötigten Speicherplatzes. Sie können diese ungefähre Berechnung verwenden, um zu überprüfen, ob Sie ausreichen freien Platz auf dem Laufwerk haben, um einen Überlauf der Datenbank zu vermeiden. Standardmäßig umfasst die Administrationsserver-Datenbank 400.000 Ereignisse. Die empfohlene Maximalgröße der Datenbank liegt bei 45 Millionen Ereignissen.

Die Anwendung überprüft die Datenbank alle 10 Minuten. Wenn die Anzahl der Ereignisse den festgelegten Höchstwert plus 10.000 erreicht, löscht die Anwendung die ältesten Ereignisse, sodass nur noch die festgelegte Höchstanzahl von Ereignissen übrig bleibt.

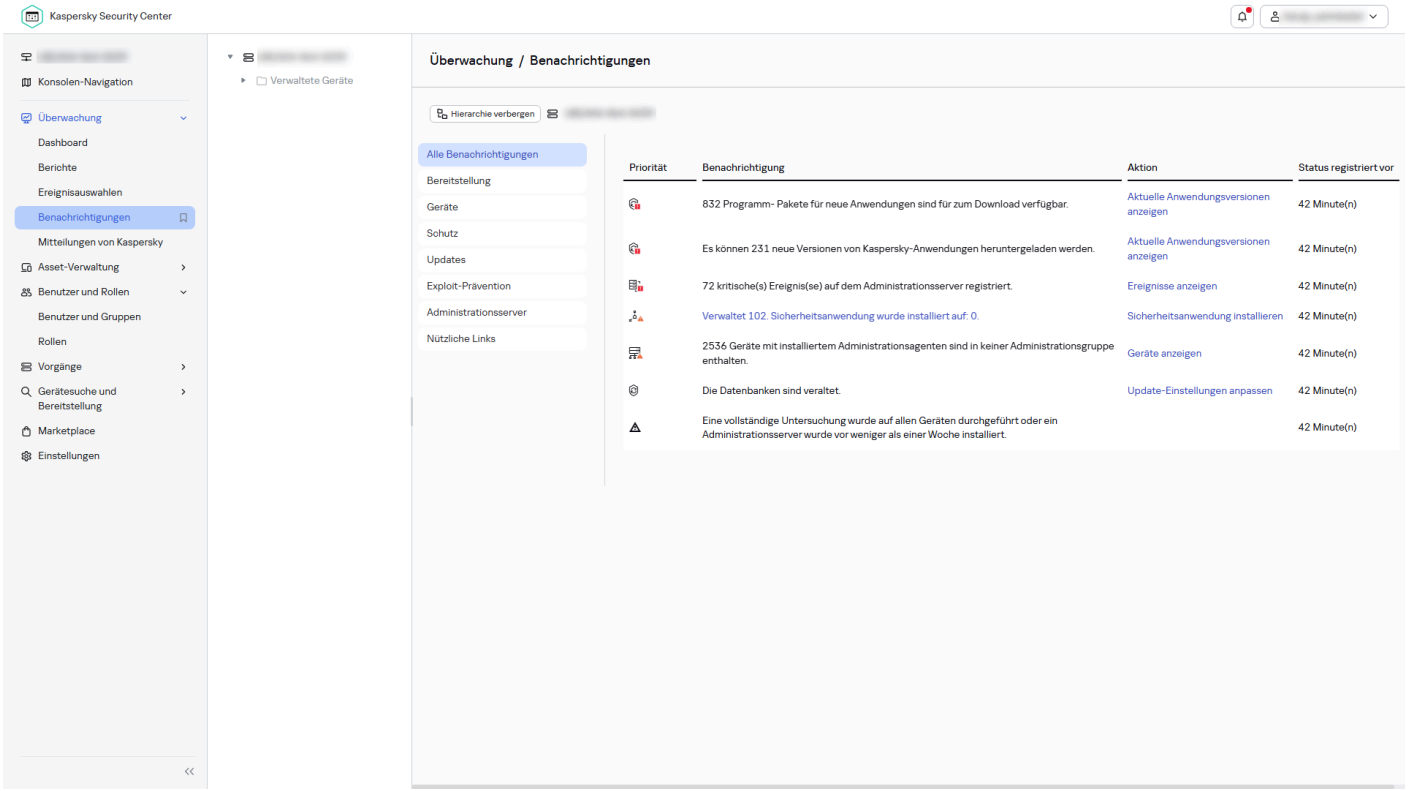
Wenn der Administrationsserver alte Ereignisse löscht, kann er keine neuen Ereignisse in der Datenbank speichern. Während diese Vorgangs werden Informationen über abgelehnte Ereignisse in das Betriebssystem-Protokoll geschrieben. Die neuen Ereignisse werden in die Warteschlange verschoben und dann in der Datenbank gespeichert, nachdem der Löschvorgang abgeschlossen wurde. Die Warteschlange für Ereignisse ist standardmäßig auf 20.000 Ereignisse beschränkt. Sie können die Beschränkung der Warteschlange anpassen, indem Sie den Wert des Flags KLEVP_MAX_POSTPONED_CNT ändern.

Benachrichtigungen und Gerätestatus

Dieser Abschnitt enthält Informationen zum Anzeigen von Benachrichtigungen, zum Konfigurieren der Zustellung von Benachrichtigungen, zum Verwenden des Gerätestatus und zum Aktivieren der Änderung von Statuswerten der Geräte.

Benachrichtigungen verwenden

Benachrichtigungen informieren Sie über Ereignisse und unterstützen Sie dabei, mithilfe empfohlener Maßnahmen oder mit Maßnahmen, die Sie als geeignet erachten, schneller auf diese Ereignisse zu reagieren.



Die Liste der Benachrichtigungen

Je nach ausgewählter Benachrichtigungsmethode, stehen die folgenden Benachrichtigungstypen zur Verfügung:

- Bildschirmbenachrichtigungen
- Benachrichtigungen per SMS
- Benachrichtigungen per E-Mail
- Benachrichtigungen per ausführbarer Datei oder Skript

Bildschirmbenachrichtigungen

Bildschirmbenachrichtigungen informieren Sie über Ereignisse, die in Ereigniskategorien gruppiert sind (*Kritisch*, *Warnung*, und *Information*).

Bildschirmbenachrichtigungen können zwei Status haben:

- *Geprüft*. Dies bedeutet, dass Sie die für diese Nachricht empfohlenen Maßnahmen durchgeführt haben oder dass Sie der Nachricht diesen Status manuell zugewiesen haben.
- *Ungeprüft*. Dies bedeutet, dass Sie die für diese Nachricht empfohlenen Maßnahmen nicht durchgeführt haben oder dass Sie der Nachricht diesen Status nicht manuell zugewiesen haben.

Standardmäßig enthält die Liste mit Benachrichtigungen die Nachrichten mit dem Status *Ungeprüft*.

Sie können Ihr Unternehmensnetzwerk durch das Anzeigen der Bildschirmbenachrichtigungen kontrollieren und in Echtzeit auf diese reagieren.

Benachrichtigungen per E-Mail, SMS und ausführbarer Datei oder Skript

Kaspersky Security Center Linux bietet die Möglichkeit, Ihr Unternehmensnetzwerk zu kontrollieren, indem Nachrichten über alle Ereignisse, die Sie als wichtig einstufen, versandt werden. Für jedes Ereignis können Sie Benachrichtigungen per E-Mail, per SMS oder durch das Starten einer ausführbaren Datei oder eines Skripts konfigurieren.

Nach dem Erhalten von Benachrichtigungen per E-Mail oder SMS können Sie entscheiden, wie Sie auf das Ereignis reagieren. Die Reaktion sollte diejenige sein, die für Ihr Unternehmensnetzwerk am geeignetsten ist. Durch den Start einer ausführbaren Datei oder eines Skripts, geben Sie eine vordefinierte Reaktion auf ein Ereignis an. Sie können den Start einer ausführbaren Datei oder eines Skripts auch als erste Reaktion auf ein Ereignis in Erwägung ziehen. Nachdem die ausführbare Datei gestartet wurde, können Sie weitere Schritte unternehmen, um auf das Ereignis zu reagieren.

Bildschirmbenachrichtigungen anzeigen

Es gibt drei Möglichkeiten, um Benachrichtigungen auf dem Bildschirm anzuzeigen:

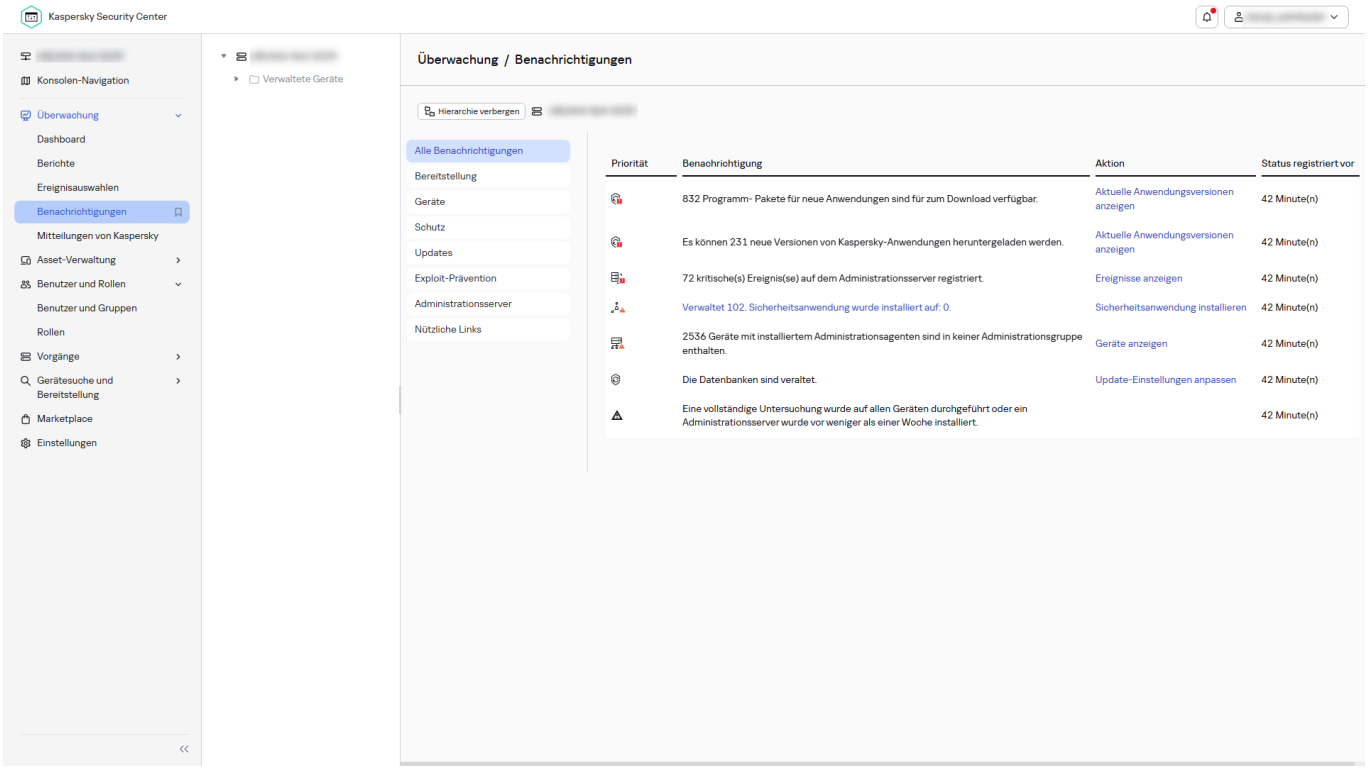
- In dem Abschnitt **Überwachung** → **Benachrichtigungen**. Hier können Sie Nachrichten über vordefinierte Kategorien anzeigen.
- In einem separaten Fenster, welches unabhängig davon, in welchem Abschnitt Sie sich gerade befinden, geöffnet werden kann. In diesem Fall können Sie Nachrichten als geprüft markieren.
- In dem Widget **Benachrichtigungen nach ausgewählter Signifikanz** im Abschnitt **Überwachung** → **Dashboard**. In dem Widget können Sie nur Nachrichten der Ereigniskategorien *Kritisch* und *Warnung* ansehen.

Sie können Aktionen ausführen, z. B. als Reaktion auf ein Ereignis.

Um Benachrichtigungen vordefinierter Kategorien anzuzeigen:

1. Gehen Sie im Hauptmenü zu **Überwachung** → **Benachrichtigungen**.

Im linken Bereich ist die Kategorie **Alle Benachrichtigungen** ausgewählt, und im rechten Bereich werden alle Benachrichtigungen angezeigt.



Die Liste der Benachrichtigungen

2. Wählen Sie im linken Bereich eine der drei Kategorien:

   - **Bereitstellung**
   - **Geräte**
   - **Schutz**
   - **Updates** (Umfasst Benachrichtigungen über zum Download verfügbare Kaspersky-Anwendungen, über heruntergeladene Updates für die Antiviren-Datenbanken sowie über Geräte (falls vorhanden), die nach einem Update des Administrationsagenten neu gestartet werden müssen)
   - **Exploit-Prävention**
   - **Administrationsserver** (Diese Kategorie umfasst Ereignisse, die nur den Administrationsserver betreffen.)
   - **Nützliche Links** (Diese Kategorie umfasst Links zu Ressourcen von Kaspersky, z. B. zum Technischen Support von Kaspersky, dem Forum von Kaspersky, der Seite für Lizenzverlängerung und der Kaspersky IT Enzyklopädie.)

Eine Liste mit Nachrichten zu den ausgewählten Kategorien wird angezeigt. Die Liste enthält Folgendes:

- Symbol, das dem Thema der Benachrichtigung entspricht: Bereitstellung, Schutz, Update, Geräteverwaltung, Exploit-Prävention, Administrationsserver.
- Ereigniskategorie der Nachricht. Angezeigt werden Nachrichten mit den folgenden Ereigniskategorien: **Kritische Benachrichtigungen**, **Warnende Benachrichtigungen**, **Informative Benachrichtigungen**. Die Benachrichtigungen in der Liste sind nach Ereigniskategorien gruppiert.
- **Benachrichtigung**. Dies beinhaltet eine Beschreibung der Nachricht.

- **Aktion**. Dies beinhaltet einen Link zu einer empfohlenen Sofortmaßnahme. Sie können beispielsweise durch klicken des Links in die Datenverwaltung wechseln und Sicherheitsanwendungen auf Geräten installieren, oder sich eine Liste mit Geräten oder Ereignissen anzeigen lassen. Nachdem die empfohlene Maßnahme für die Nachricht durchgeführt wurde, wird der Nachricht der Status *Geprüft* zugewiesen.

- **Status registriert vor**. Dies beinhaltet die Anzahl der vergangenen Tage und Stunden, seit die Nachricht auf dem Administrationsserver registriert wurde.

Um Bildschirmbenachrichtigungen nach Ereigniskategorien in einem separaten Fenster anzuzeigen:

1. Klicken Sie in der rechten oberen Ecke der Kaspersky Security Center Web Console auf das Flaggen-Symbol ( ).

   Wenn das Flaggen-Symbol einen roten Punkt besitzt, existieren Nachrichten, die noch nicht gelesen wurden.

   Es öffnet sich ein Fenster mit der Liste von Nachrichten. Standardmäßig ist die Registerkarte **Alle Benachrichtigungen** ausgewählt und die Nachrichten sind nach Ereigniskategorie gruppiert: *Kritisch*, *Warnung*, und *Information*.

2. Wählen Sie die Registerkarte **System** aus.

   Die Liste der Nachrichten mit den Ereigniskategorien *Kritisch* ( ) und *Warnung* ( ) wird angezeigt. Die Liste der Nachrichten enthält Folgendes:

   - Eine Farbmarkierung. Kritische Benachrichtigungen sind rot markiert. Warnende Benachrichtigungen sind gelb markiert.
   - Symbol, welches das Thema der Benachrichtigung angibt: Bereitstellung ( ), Schutz ( ), Update ( ), Geräteverwaltung ( ), Exploit-Prävention ( ), Administrationsserver ( ).
   - Eine Beschreibung der Nachricht.
   - Flaggen-Symbol. Das Flaggen-Symbol ist grau, wenn Benachrichtigungen der Status *Nicht gelesen* zugewiesen wurden. Wenn Sie das graue Flaggen-Symbol auswählen und einer Nachricht den Status *Gelesen* zuweisen, ändert sich die Farbe des Symbols zu weiß.
   - Link zur empfohlenen Maßnahme. Wenn Sie auf den Link klicken und anschließend die empfohlene Maßnahme durchführen, erhält die Nachricht den Status *Geprüft*.
   - Die Anzahl der vergangenen Tage seit die Nachricht auf dem Administrationsserver registriert wurde.

3. Wählen Sie die Registerkarte **Mehr** aus.

   Die Liste der Benachrichtigungen mit der Ereigniskategorie *Information* wird angezeigt.

   Der Aufbau der Liste ist identisch mit dem der Liste für die Registerkarte **System** (siehe oben). Der einzige Unterschied ist die fehlende Farbmarkierung.

Sie können Benachrichtigungen nach dem Datumsintervall, in welchem sie auf dem Administrationsserver registriert wurden, filtern. Benutzen Sie das Kontrollkästchen **Filter anzeigen** um den Filter zu verwalten.

Um Bildschirmbenachrichtigungen im Widget anzuzeigen:

1. Wählen Sie im Abschnitt **Dashboard** den Punkt **Widget hinzufügen oder wiederherstellen**.
2. Klicken Sie in dem sich öffnenden Fenster auf die Kategorie **Andere**, wählen Sie das Widget **Benachrichtigungen nach ausgewählter Signifikanz** aus, und klicken Sie auf Hinzufügen.

   Das Widget erscheint jetzt auf der Registerkarte **Dashboard**. Standardmäßig zeigt das Widget Benachrichtigungen mit der Ereigniskategorie *Kritisch* an.

   Sie können in dem Widget auf die Schaltfläche **Einstellungen** klicken und die Einstellungen des Widgets ändern, um Nachrichten mit der Ereigniskategorie *Warnung* anzuzeigen. Oder Sie können mittels **Benachrichtigungen nach ausgewählter Signifikanz**, ein weiteres Widget mit der Ereigniskategorie *Warnung* hinzufügen.

   Die Liste der Benachrichtigungen ist im Widget in seiner Größe eingeschränkt und enthält zwei Nachrichten. Diese zwei Nachrichten entsprechen den zwei neuesten Ereignissen.

Im Widget enthält die Liste der Nachrichten Folgendes:

- Symbol, das dem Thema der Benachrichtigung entspricht: Bereitstellung (), Schutz (), Update (), Geräteverwaltung (), Exploit-Prävention (), Administrationsserver ().
- Eine Beschreibung der Nachricht mit einem Link zur empfohlenen Maßnahme. Wenn Sie auf den Link klicken und anschließend eine empfohlene Maßnahme durchführen, erhält die Nachricht den Status *Geprüft*.
- Die Anzahl der vergangenen Tage oder Stunden seit die Nachricht auf dem Administrationsserver registriert wurde.
- Ein Link zu weiteren Benachrichtigungen. Durch das Anklicken des Links gelangen Sie in den Unterabschnitt **Benachrichtigungen** des Abschnitts **Überwachung**.

Über die Varianten für den Gerätestatus

Kaspersky Security Center Linux weist jedem verwalteten Gerät einen Status zu. Der jeweilige Status hängt davon ab, ob die vom Benutzer definierten Bedingungen erfüllt sind. Wenn Kaspersky Security Center Linux einem Gerät einen Status zuweist, wird für bestimmte Bedingungen das Sichtbarkeits-Flag des Gerätes im Netzwerk berücksichtigt (siehe folgende Tabelle). Beispiel: Wenn einem verwalteten Gerät der Status *Kritisch* zugewiesen wurde, da die Bedingung *Die Datenbanken sind veraltet* erfüllt ist und für das Gerät später das Sichtbarkeits-Flag gesetzt wurde, erhält das Gerät den Status *OK*. Wenn Kaspersky Security Center Linux ein Gerät innerhalb von zwei Stunden nicht im Netzwerk findet, wird das Sichtbarkeits-Flag des Gerätes auf *Nicht sichtbar* gesetzt.

Es gibt folgende Statusvarianten:

- *Kritisch* oder *Kritisch/Sichtbar*
- *Warnung* oder *Warnung/Sichtbar*
- *OK* oder *OK/Sichtbar*

Die folgende Tabelle enthält die erforderlichen Standardbedingungen, nach denen einem Gerät der Status *Kritisch* oder *Warnung* zugewiesen wird, sowie alle möglichen Werte.

Bedingungen für das Zuweisen der Status an das Gerät

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Sicherheitsanwendung ist nicht installiert	Auf dem Gerät ist der Administrationsagent installiert, aber es wurde keine Sicherheitsanwendung installiert.	• Umschalter aktiviert. • Umschalter deaktiviert.

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Zu viele Viren gefunden	Auf dem Gerät wurden als Ergebnis der Ausführung einer Aufgabe zur Virensuche (beispielsweise der Aufgabe zur Schadsoftware-Untersuchung) mehrere Viren gefunden, und die Anzahl der gefundenen Viren übersteigt den angegebenen Wert.	Über 0.
Die Stufe des Echtzeitschutzes unterscheidet sich von der Stufe, die der Administrator festgelegt hat	Das Gerät ist im Netzwerk sichtbar, aber die Stufe des Echtzeitschutzes unterscheidet sich von der Stufe, die vom Administrator (in der Bedingung) für den Gerätestatus eingestellt wurde.	• Beendet. • Angehalten. • Wird ausgeführt.
Die letzte Schadsoftware-Untersuchung liegt lange zurück	Das Gerät ist im Netzwerk sichtbar und es wurde eine Sicherheitsanwendung auf dem Gerät installiert, aber es wurde weder die Aufgabe zur *Schadsoftware-Untersuchung*, noch die Aufgabe zur lokalen Untersuchung innerhalb des angegebenen Zeitintervalls ausgeführt. Die Bedingung gilt nur für Geräte, die vor mehr als sieben Tagen zur Administrationsserver-Datenbank hinzugefügt wurden.	Über 1 Tag.
Die Datenbanken sind veraltet	Das Gerät ist im Netzwerk sichtbar und eine Sicherheitsanwendung wurde auf dem Gerät installiert, aber die Antiviren-Datenbanken wurden auf diesem Gerät nicht innerhalb des angegebenen Zeitintervalls aktualisiert. Die Bedingung gilt nur für Geräte, die vor mehr als einem Tag zur Administrationsserver-Datenbank hinzugefügt wurden.	Über 1 Tag.
Die letzte Verbindung liegt lange zurück	Der Administrationsagent ist auf dem Gerät installiert, es wurde allerdings nicht innerhalb des angegebenen Zeitintervalls mit dem Administrationsserver verbunden, da es deaktiviert ist.	Über 1 Tag.
Aktive Bedrohungen wurden erkannt	Die Anzahl der unbearbeiteten Objekte im Ordner **Aktive Bedrohungen** übersteigt den angegebenen Wert.	Über 0 Elemente.
Neustart erforderlich seit	Das Gerät ist im Netzwerk sichtbar, aber eine Anwendung erfordert einen Neustart des Geräts. Der Zeitpunkt der Anfrage liegt länger zurück, als im Zeitintervall angegeben.	Über 0 Minuten.
Grund des Neustarts	Das Gerät ist im Netzwerk sichtbar, aber eine Anwendung erfordert aus einem der ausgewählten Gründe einen Neustart des Geräts.	• Unbekannter Ursache • Anwendung wird erst nach Neustart ausgeführt • Um das Update abzuschließen, ist ein Neustart erforderlich; die Anwendung ist jedoch funktionsfähig • Zum Start des Updates ist ein Neustart erforderlich • Zum Abschließen der Untersuchung oder Desinfektion ist ein Neustart erforderlich • Um die Remote-Installation bzw. -Deinstallation abzuschließen, ist ein Neustart erforderlich • Abschließen der Datenverschlüsselung auf der Festplatte
Es sind inkompatible Anwendungen installiert	Das Gerät ist im Netzwerk sichtbar, aber infolge der Inventarisierung der Software durch den Administrationsagenten wurden auf dem Gerät inkompatible Anwendungen gefunden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Es wurden Schwachstellen in Programmen erkannt	Das Gerät ist im Netzwerk sichtbar und der Administrationsagent ist auf dem Gerät installiert, aber die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* hat in den Programmen auf dem Gerät Schwachstellen mit der angegebenen Signifikanz gefunden.	• Kritisch. • Hoch. • Normal. • Ignorieren, wenn die Schwachstelle nicht geschlossen werden kann. • Ignorieren, wenn das Update für die Installation bestimmt wurde.
Lizenz abgelaufen	Das Gerät ist im Netzwerk sichtbar, aber die Lizenz ist abgelaufen.	• Umschalter deaktiviert. • Umschalter aktiviert.
Die Lizenz läuft bald ab	Das Gerät ist im Netzwerk sichtbar, aber die Lizenz auf dem Gerät läuft in weniger als der angegebenen Anzahl an Tagen ab.	Über 0 Tage.

Bedingung	Beschreibung der Bedingung	Mögliche Werte
Die letzte Suche nach Windows-Updates liegt lange zurück	Das Gerät ist im Netzwerk sichtbar, aber die Aufgabe *Finden von Schwachstellen und erforderlichen Updates* wurde nicht innerhalb des angegebenen Zeitintervalls ausgeführt.	Über 1 Tag.
Ungültiger Verschlüsselungsstatus	Der Administrationsagent ist auf dem Gerät installiert, aber das Ergebnis der Verschlüsselung des Geräts entspricht dem angegebenen Wert.	• Entspricht nicht der Richtlinie aufgrund der Ablehnung durch den Benutzer (nur für externe Geräte). • Entspricht nicht der Richtlinie wegen eines Fehlers. • Bei der Übernahme der Richtlinie – Neustart erforderlich. • Es wurde keine Verschlüsselungsrichtlinie festgelegt. • Nicht unterstützt. • Bei der Übernahme der Richtlinie.
Die Einstellungen des mobilen Geräts entsprechen nicht der Richtlinie	Die Einstellungen des mobilen Geräts unterscheiden sich von den in der Richtlinie von Kaspersky Endpoint Security für Android festgelegten Einstellungen beim Ausführen der Untersuchung der Übereinstimmungsregeln.	• Umschalter deaktiviert. • Umschalter aktiviert.
Es wurden unbearbeitete Sicherheitsprobleme erkannt	Auf dem Gerät sind unbearbeitete Sicherheitsvorfälle vorhanden. Sicherheitsvorfälle können sowohl automatisch mithilfe von auf dem Client-Gerät installierten verwalteten Kaspersky-Anwendungen als auch manuell durch den Administrator erstellt werden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Gerätestatus wird durch Anwendung bestimmt	Der Gerätestatus wird von der verwalteten Anwendung bestimmt. Verwaltete Geräte können einen Status besitzen, der von den verwalteten Anwendungen unabhängig von den Einstellungen von Kaspersky Security Center Linux bestimmt wird. Wenn der Status zu einem der Werte zurückkehrt, die durch Kaspersky Security Center Linux bestimmt werden, weist der Administrationsserver einem verwalteten Gerät den kritischsten Status zu, der von der verwalteten Anwendung zurückgegeben und vom Administrationsserver zugewiesen wurde. Statuswerte, die von verwalteten Anwendungen bestimmt werden, besitzen Beschreibungen, die ebenfalls von den verwalteten Anwendungen stammen. Sie können diese Beschreibungen in der Liste der verwalteten Geräte in der Spalte **Statusbeschreibung**.	• Umschalter ist deaktiviert. • Umschalter ist aktiviert.
Kein Platz auf dem Datenträger des Geräts	Der freie Speicherplatz auf dem Datenträger ist kleiner als der angegebene Wert oder das Gerät konnte nicht mit dem Administrationsserver synchronisiert werden. Der Status *Kritisch* oder *Warnung* wird in den Status *OK* geändert, wenn das Gerät erfolgreich mit dem Administrationsserver synchronisiert wird und der freie Speicherplatz auf dem Gerät dem angegebenen Wert entspricht oder diesen überschreitet.	Über 0 MB.
Das Gerät wird nicht mehr verwaltet	Bei der Gerätesuche ist das Gerät im Netzwerk sichtbar, aber es sind mehr als drei Synchronisierungsversuche mit dem Administrationsserver fehlgeschlagen.	• Umschalter deaktiviert. • Umschalter aktiviert.
Der Schutz ist deaktiviert	Das Gerät ist im Netzwerk sichtbar, aber die Sicherheitsanwendung auf dem Gerät ist länger deaktiviert, als im Zeitintervall angegeben. In diesem Fall lautet der Status der Sicherheitsanwendung *Angehalten* oder *Fehler* und unterscheidet sich von den folgenden Statuswerten *Wird gestartet*, *Wird ausgeführt* oder *Wird angehalten*.	Über 0 Minuten.
Die Sicherheitsanwendung wurde nicht gestartet	Das Gerät ist im Netzwerk sichtbar und eine Sicherheitsanwendung ist auf dem Gerät installiert, wurde aber nicht gestartet.	• Umschalter deaktiviert. • Umschalter aktiviert.

Kaspersky Security Center Linux ermöglicht es, den Status eines Gerätes in einer Administrationsgruppe unter bestimmten Bedingungen automatisch zu ändern. Bei Erfüllung der festgelegten Bedingungen wird dem Client-Gerät einer der folgenden Statuswerte verliehen: *Kritisch* oder *Warnung*. Sind die festgelegten Bedingungen nicht erfüllt, so erhält das Client-Gerät den Status *OK*.

Verschiedenen Werten einer einzelnen Bedingung können verschiedene Statusvarianten entsprechen. Beispiele: Wenn die Bedingung **Die Datenbanken sind veraltet** den Wert **Über 3 Tage** besitzt, erhält das Client-Gerät standardmäßig den Status *Warnung* und für den Wert **Über 7 Tage** wird ihm der Status *Kritisch* zugewiesen.

Wenn Sie ein Upgrade für Kaspersky Security Center Linux durchführen und es von einer früheren Version aktualisieren, bleiben die Werte der Bedingung **Die Datenbanken sind veraltet**, bei denen dem Gerät der Status *Warnung* oder *Kritisch* zugewiesen wird, identisch.

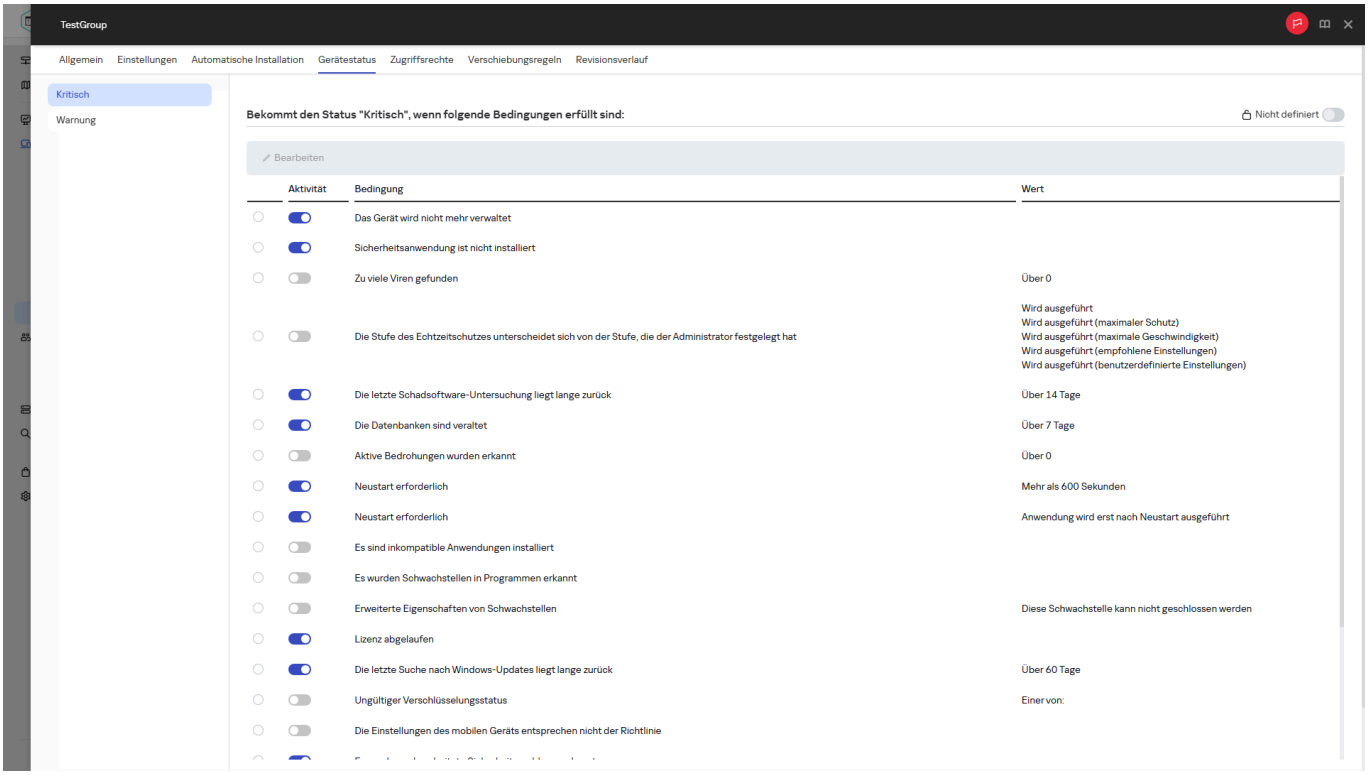
Wechsel der Statuswerte von Geräten konfigurieren

Sie können die Bedingungen ändern, um einem Gerät den Status *Kritisch* oder *Warnung* zuzuweisen.

Um die Änderungen des Gerätestatus auf Kritisch zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Gruppenhierarchie**.
2. Wechseln Sie auf eine der folgenden Arten zu den Eigenschaften der Administrationsgruppe, für welche Sie den Gerätestatus ändern möchten:
   - Klicken Sie auf den Namen der Administrationsgruppe.
   - Klicken Sie im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen**. Bewegen Sie im neuen Navigationsbereich den Mauszeiger über den Namen der gewünschten Gruppe und klicken Sie anschließend auf das Einstellungssymbol (⚙).

   Das Eigenschaftenfenster der übergeordneten Administrationsgruppe wird geöffnet.
3. Klicken Sie im Eigenschaftsfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Kritisch** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Bekommt den Status "Kritisch" zugewiesen, wenn folgende Bedingungen erfüllt sind** die Bedingung zum Umschalten eines Geräts in den Status *Kritisch*.



Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.
8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.
   Es können nicht für alle Bedingungen Werte festgelegt werden.
9. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Kritisch*.

Um die Änderungen des Gerätestatus auf Warnung zu aktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Gruppenhierarchie**.
2. Klicken Sie in der angezeigten Liste der Gruppen auf den Link mit dem Namen der Gruppe, für die Sie den Wechsel der Gerätestatus ändern möchten.
3. Klicken Sie im daraufhin geöffneten Eigenschaftenfenster auf die Registerkarte **Gerätestatus**.
4. Wählen Sie im linken Fensterbereich die Option **Warnung** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Bekommt den Status "Warnung" zugewiesen, wenn folgende Bedingungen erfüllt sind** die Bedingung zum Umschalten eines Geräts in den Status *Warnung*.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

6. Aktivieren Sie das Optionsfeld neben der Bedingung in der Liste.
7. Klicken Sie in der oberen linken Ecke der Liste auf die Schaltfläche **Bearbeiten**.
8. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.
   Es können nicht für alle Bedingungen Werte festgelegt werden.
9. Klicken Sie auf die Schaltfläche **OK**.

Sind die festgelegten Bedingungen erfüllt, so erhält das verwaltete Gerät den Status *Warnung*.

Einstellungen für das Versenden von Benachrichtigungen anpassen

Sie können die Benachrichtigung über Ereignisse, die in Kaspersky Security Center Linux auftreten, konfigurieren. Je nach ausgewählter Benachrichtigungsmethode, stehen die folgenden Benachrichtigungstypen zur Verfügung:

- E-Mail: Wenn Ereignisse auftreten, sendet Kaspersky Security Center Linux Benachrichtigungen an die angegebenen E-Mail-Adressen.
- SMS: Wenn Ereignisse auftreten, sendet Kaspersky Security Center Linux Benachrichtigungen an die angegebenen Telefonnummern.
- Ausführbare Datei: Wählen Sie die ausführbare Datei, die auf dem Administrationsserver gestartet wird, wenn ein Ereignis eintritt.

Um den Versand von Benachrichtigungsereignissen in Kaspersky Security Center Linux zu konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Klicken Sie auf den Abschnitt **Benachrichtigung**, und wählen Sie im rechten Bereich die Registerkarte für die gewünschte Benachrichtigungsmethode:

   - **E-Mail**

     Auf der Registerkarte **E-Mail** können Sie die Ereignisprotokollierung per E-Mail konfigurieren.

     Geben Sie im Feld **SMTP-Server** die Adressen der Mail-Server durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

     - IPv4- oder IPv6-Adresse
     - DNS-Name des SMTP-Servers

     Geben Sie im Feld **Port des SMTP-Servers** die Nummer des Kommunikationsports auf dem SMTP-Server an. Standardmäßig wird Portnummer 25 verwendet.

     Wenn Sie die Option **MX-Lookup per DNS-Server verwenden** aktivieren, können Sie mehrere MX-Einträge von IP-Adressen für denselben DNS-Namen des SMTP-Servers verwenden. Der gleiche DNS-Name kann mehrere MX-Einträge mit unterschiedlichen Prioritäten für das Empfangen von E-Mail-Nachrichten enthalten. Der Administrationsserver versucht, entsprechend der Priorität der MX-Einträge, die E-Mail-Nachrichten in aufsteigender Reihenfolge an den SMTP-Server zu senden.

     > Wenn Sie die Option **MX-Lookup per DNS-Server verwenden** aktivieren und die Verwendung von TLS-Einstellungen deaktivieren, ist es empfehlenswert, die DNSSEC-Einstellungen auf Ihrem Servergerät als zusätzliche Schutzmaßnahme beim Senden von E-Mail-Nachrichten zu verwenden.

     Wenn Sie die Option **ESMTP-Authentifizierung verwenden** aktivieren, können Sie die ESMTP-Authentifizierungseinstellungen in den Feldern **Benutzername** und **Kennwort** angeben. Standardmäßig ist die Option deaktiviert und die ESMTP-Authentifizierungseinstellungen sind nicht verfügbar.

     Sie können die TLS-Einstellungen einer Verbindung mit einem SMTP-Server angeben:

     - **Kein TLS verwenden**

Sie können diese Option auswählen, wenn Sie die Verschlüsselung von E-Mail-Nachrichten deaktivieren möchten.

- **TLS verwenden, wenn dies vom SMTP-Server unterstützt wird**

Sie können diese Option auswählen, wenn Sie eine TLS-Verbindung zu einem SMTP-Server verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, verbindet der Administrationsserver den SMTP-Server ohne TLS zu verwenden.

- **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen**

Sie können diese Option auswählen, wenn Sie Authentifizierungseinstellungen von TLS verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, kann der Administrationsserver keine Verbindung zu dem SMTP-Server herstellen.

Es wird empfohlen, diese Option für einen besseren Schutz der Verbindung mit einem SMTP-Server zu verwenden. Wenn Sie diese Option auswählen, können Sie Authentifizierungseinstellungen für eine TLS-Verbindung festlegen.

Wenn Sie den Wert **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen** ausgewählt haben, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie ein Zertifikat für die Client-Authentifizierung an dem SMTP-Server angeben.

Sie können Zertifikate für eine TLS-Verbindung angeben, indem Sie auf den Link **Zertifikate angeben** klicken:

- Geben Sie eine Datei mit SMTP-Server-Zertifikat an:

Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von eine vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei auf den Administrationsserver hochladen. Kaspersky Security Center Linux prüft, ob das Zertifikat eines SMTP-Servers auch von einer vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center Linux kann keine Verbindung zu einem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von eine vertrauenswürdigen Zertifizierungsstelle kommt.

- Geben Sie die Datei des Client-Zertifikats an:

Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen Zertifizierungsstelle. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

- X-509-Zertifikat:

Sie müssen eine Datei mit dem Zertifikat und eine Datei mit dem privaten Schlüssel angeben. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Laden der Dateien ist spielt keine Rolle. Wenn beide Dateien geladen sind, müssen Sie das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

- pkcs12-Container:

Sie müssen eine einzelne Datei hochladen, die das Zertifikat und seinen privaten Schlüssel enthält. Wenn die Datei geladen ist, müssen Sie anschließend das Kennwort zum Entschlüsseln des privaten Schlüssels angeben. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

Wenn Sie auf die Schaltfläche **Testnachricht senden** klicken, können Sie prüfen, ob die Benachrichtigungen korrekt angepasst sind: Die Anwendung sendet eine Testnachricht an die von Ihnen angegebenen E-Mail-Adressen.

Geben Sie im Feld **Empfänger (E-Mail-Adressen)** die E-Mail-Adressen an, an welche die Anwendung Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen.

Geben Sie im Feld **Betreff** den Betreff der E-Mail an. Sie können dieses Feld leer lassen.

Wählen Sie in der Dropdown-Liste **Betreffsvorlage** die Vorlage für Ihren Betreff aus. Eine durch die ausgewählte Vorlage bestimmte Variable wird automatisch in das Feld **Betreff** eingefügt. Sie können einen E-Mail-Betreff erstellen, indem Sie mehrere Betreffsvorlagen auswählen.

Geben Sie im Feld **E-Mail-Adresse des Absenders: Wenn diese Einstellung nicht angegeben ist, wird stattdessen die Empfängeradresse verwendet. Achtung: Es wird nicht empfohlen, eine fiktive E-Mail-Adresse zu verwenden** die E-Mail-Adresse des Absenders an. Wenn Sie dieses Feld leer lassen, wird standardmäßig die Empfängeradresse verwendet. Wir raten davon ab, fingierte E-Mail-Adressen zu verwenden.

Das Feld **Benachrichtigungstext** enthält Standard-Text mit der Information zum Ereignis, der beim Eintreten des Ereignisses versendet wird. Dieser Text enthält Platzhalter für den Ereignisnamen, den Gerätenamen und den Namen der Domäne. Sie können den Text der Meldung bearbeiten und weitere Platzhalter mit relevanten Informationen zum Ereignis hinzufügen.

> Wenn der Benachrichtigungstext ein Prozentzeichen (%) enthält, muss es zweimal hintereinander angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

Wenn Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren** klicken, können Sie die maximale Anzahl an Benachrichtigungen angeben, welche die Anwendung innerhalb des angegebenen Zeitintervalls versenden darf.

- **SMS**

Auf der Registerkarte **SMS** können Sie den Versand von SMS-Benachrichtigungen zu verschiedenen Ereignissen an ein Mobiltelefon anpassen. SMS-Nachrichten werden über ein Mail-Gateway gesendet.

Geben Sie im Feld **SMTP-Server** die Adressen der Mail-Server durch Semikolon getrennt an. Sie können folgende Parameterwerte verwenden:

- IPv4- oder IPv6-Adresse
- DNS-Name des SMTP-Servers

Geben Sie im Feld **Port des SMTP-Servers** die Nummer des Kommunikationsports auf dem SMTP-Server an. Standardmäßig wird Portnummer 25 verwendet.

Wenn die Option **ESMTP-Authentifizierung verwenden** aktiviert ist, können Sie die ESMTP-Authentifizierungseinstellungen in den Feldern **Benutzername** und **Kennwort** angeben. Standardmäßig ist die Option deaktiviert und die ESMTP-Authentifizierungseinstellungen sind nicht verfügbar.

Sie können die TLS-Einstellungen einer Verbindung mit einem SMTP-Server angeben:

- **Kein TLS verwenden**

Sie können diese Option auswählen, wenn Sie die Verschlüsselung von E-Mail-Nachrichten deaktivieren möchten.

- **TLS verwenden, wenn dies vom SMTP-Server unterstützt wird**

Sie können diese Option auswählen, wenn Sie eine TLS-Verbindung zu einem SMTP-Server verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, verbindet der Administrationsserver den SMTP-Server ohne TLS zu verwenden.

- **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen**

Sie können diese Option auswählen, wenn Sie Authentifizierungseinstellungen von TLS verwenden möchten. Wenn der SMTP-Server kein TLS unterstützt, kann der Administrationsserver keine Verbindung zu dem SMTP-Server herstellen.

Es wird empfohlen, diese Option für einen besseren Schutz der Verbindung mit einem SMTP-Server zu verwenden. Wenn Sie diese Option auswählen, können Sie Authentifizierungseinstellungen für eine TLS-Verbindung festlegen.

Wenn Sie den Wert **Immer TLS verwenden, das Serverzertifikat auf Gültigkeit überprüfen** ausgewählt haben, können Sie ein Zertifikat für die Authentifizierung des SMTP-Servers angeben und auswählen, ob Sie die Kommunikation über eine beliebige Version von TLS oder nur über TLS 1.2 oder höher aktivieren möchten. Außerdem können Sie ein Zertifikat für die Client-Authentifizierung an dem SMTP-Server angeben.

Sie können die Zertifikatsdatei des SMTP-Servers angeben, indem Sie auf den Link **Zertifikate angeben** klicken. Sie können eine Datei bekommen, die eine Liste mit Zertifikaten von eine vertrauenswürdigen Zertifizierungsstelle enthält, und diese Datei auf den Administrationsserver hochladen. Kaspersky Security Center Linux prüft, ob das Zertifikat eines SMTP-Servers auch von einer vertrauenswürdigen Zertifizierungsstelle signiert ist oder nicht. Kaspersky Security Center Linux kann keine Verbindung zu einem SMTP-Server herstellen, wenn das Zertifikat des SMTP-Servers nicht von eine vertrauenswürdigen Zertifizierungsstelle kommt.

Geben Sie im Feld **Empfänger (E-Mail-Adressen)** die E-Mail-Adressen an, an die das Programm Benachrichtigungen senden soll. Sie können in diesem Feld mehrere Adressen angeben, indem Sie diese durch Semikolons trennen. Die Benachrichtigungen werden an die Telefonnummern gesendet, die den angegebenen E-Mail-Adressen zugewiesen sind.

Geben Sie im Feld **Betreff** den Betreff der E-Mail an.

Wählen Sie in der Dropdown-Liste **Betreffsvorlage** die Vorlage für Ihren Betreff aus. Eine Variable entsprechend der ausgewählten Vorlage wird in das Feld **Betreff** eingefügt. Sie können einen E-Mail-Betreff erstellen, indem Sie mehrere Betreffsvorlagen auswählen.

Geben Sie im Feld **E-Mail-Adresse des Absenders: Wenn diese Einstellung nicht angegeben ist, wird stattdessen die Empfängeradresse verwendet. Achtung: Es wird nicht empfohlen, eine fiktive E-Mail-Adresse zu verwenden** die E-Mail-Adresse des Absenders an. Wenn Sie dieses Feld leer lassen, wird standardmäßig die Empfängeradresse verwendet. Wir raten davon ab, fingierte E-Mail-Adressen zu verwenden.

Geben Sie im Feld **Telefonnummern der SMS-Nachrichtenempfänger** die Mobiltelefonnummern der Empfänger der SMS-Benachrichtigungen ein.

Geben Sie im Feld **Benachrichtigungstext** den Text mit der Information zum Ereignis ein, der beim Eintreten des Ereignisses versendet wird. Dieser Text kann Platzhalter für den Ereignisnamen, den Gerätenamen und den Namen der Domäne enthalten.

Wenn der Benachrichtigungstext ein Prozentzeichen (%) enthält, muss es zweimal hintereinander angegeben werden, damit die Nachricht versendet werden kann. Beispielsweise "Die Prozessor-Auslastung liegt bei 100%%".

Klicken Sie auf **Testnachricht senden**, um zu prüfen, ob Sie die Benachrichtigungen korrekt konfiguriert haben: Die Anwendung sendet eine Testnachricht an die von Ihnen angegebenen Empfänger.

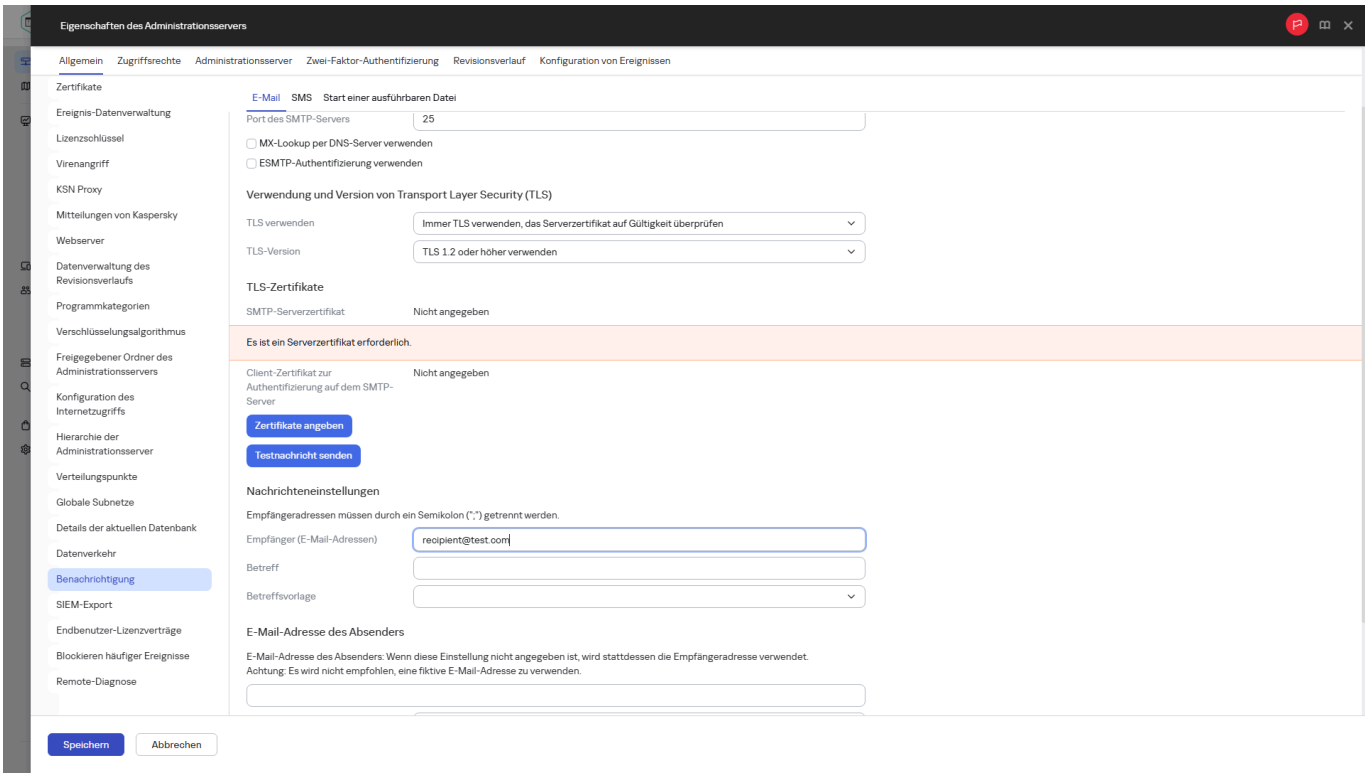
Klicken Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren**, um die maximale Anzahl an Benachrichtigungen anzugeben, welche die Anwendung während des angegebenen Zeitintervalls versenden darf.

- **Start einer ausführbaren Datei**

  Wenn diese Methode der Zustellung von Benachrichtigungen ausgewählt ist, können Sie im Eingabefeld die Anwendung angeben, die gestartet wird, sobald ein Ereignis eintritt.

Geben Sie im Feld **Ausführbare Datei, die auf dem Administrationsserver gestartet wird, wenn ein Ereignis eintritt** den Ordner und den Namen der auszuführenden Datei an. Bevor Sie die Datei angeben, bereiten Sie die diese vor und geben Sie die Platzhalter an die für die Ereignisdetails stehen, die in der Nachricht gesendet werden sollen. Der von Ihnen angegebene Ordner und die Datei müssen sich auf dem Administrationsserver befinden.

Wenn Sie auf den Link **Beschränkung für die Anzahl der Benachrichtigungen konfigurieren** klicken, können Sie die maximale Anzahl an Benachrichtigungen angeben, die das Programm innerhalb des angegebenen Zeitintervalls versenden darf.



Auswählen der Benachrichtigungsmethode

3. Definieren Sie auf der Registerkarte die Benachrichtigungseinstellungen.

4. Klicken Sie auf die Schaltfläche **OK**, um das Eigenschaftenfenster des Administrationsservers zu schließen.

Die gespeicherten Einstellungen für die Zustellung von Benachrichtigungen werden auf alle Ereignisse angewendet, die in Kaspersky Security Center Linux auftreten.

Für die Einstellungen des Administrationsservers, einer Richtlinie oder der Anwendung können Sie im Abschnitt **Konfiguration von Ereignissen** die Benachrichtigungseinstellungen für bestimmte Ereignisse überschreiben.

Verteilung von Benachrichtigungen prüfen

Um zu überprüfen, ob Ereignisbenachrichtigungen versendet werden, verwendet die Anwendung eine Benachrichtigung über den Fund des Eicar-Testvirus auf den Client-Geräten.

Um die Verteilung von Benachrichtigungen über Ereignisse zu überprüfen, gehen Sie wie folgt vor:

1. Halten Sie auf einem Client-Computer den Echtzeitschutz für das Dateisystem an und kopieren Sie den Eicar-Testvirus auf das Client-Gerät. Aktivieren Sie den Echtzeitschutz für das Dateisystem wieder.

2. Starten Sie eine Untersuchungsaufgabe für die Client-Geräte in einer Administrationsgruppe oder für eine Reihe von Geräten, zu denen das Client-Gerät mit dem Eicar-Testvirus gehört.

   Wenn die Untersuchungsaufgabe richtig konfiguriert ist, wird der Testvirus gefunden. Wurden die Einstellungen für Benachrichtigungen richtig angepasst, empfangen Sie eine Meldung über den gefundenen Virus.

Um einen Eintrag für die Erkennung des Testvirus zu öffnen:

1. Gehen Sie im Hauptmenü zu **Überwachung** → **Ereignisauswahlen**.

2. Klicken Sie auf den Namen der Auswahl **Letzte Ereignisse**.

   Im angezeigten Fenster wird die Benachrichtigung über den Testvirus angezeigt.

Der Eicar-Testvirus enthält keinen Programmcode, der Ihrem Gerät Schaden zufügen könnte. Die Sicherheitsanwendungen der meisten Hersteller identifizieren ihn aber als Virus. Der Testvirus steht auf der offiziellen EICAR-Website zum Download bereit.

Benachrichtigung über Ereignisse mithilfe einer ausführbaren Datei

Kaspersky Security Center Linux bietet die Möglichkeit, den Administrator durch den Start einer ausführbaren Datei über Ereignisse auf den Client-Geräten zu benachrichtigen. Diese ausführbare Datei muss eine weitere ausführbare Datei mit Umgebungsvariablen für das Ereignis enthalten, die dem Administrator übermittelt werden müssen (siehe Tabelle unten).

Umgebungsvariablen zur Beschreibung des Ereignisses

Umgebungsvariable	Beschreibung der Umgebungsvariablen
$SEVERITY	Signifikanz des Ereignisses. Mögliche Werte: • **Information** • **Warnung** • **Fehler** • **Kritisch**
$COMPUTER	Name des Geräts, auf dem das Ereignis eingetreten ist. Die maximale Länge des Gerätenamens beträgt 256 Zeichen.
$DOMAIN	Domänenname des Geräts, auf dem das Ereignis eingetreten ist.
$EVENT	Name des Ereignistyps. Die maximale Länge des Namens des Ereignistyps beträgt 50 Zeichen.
$DESCR	Ereignisbeschreibung. Die maximale Länge der Beschreibung beträgt 1000 Zeichen.
$RISE_TIME	Zeitpunkt der Ereigniserstellung.
$KLCSAK_EVENT_TASK_DISPLAY_NAME	Aufgabenname. Die maximale Länge des Aufgabennamens beträgt 100 Zeichen.
$KL_PRODUCT	Name der Anwendung.
$KL_VERSION	Versionsnummer der Anwendung.

Umgebungsvariable	Beschreibung der Umgebungsvariablen
$KLCSAK_EVENT_SEVERITY_NUM	Signifikanzkennzahl des Ereignisses. Mögliche Werte: • 1 – **Information** • 2 – **Warnung** • 3 – **Fehler** • 4 – **Kritisch**
$HOST_IP	IP-Adresse des Geräts, auf dem das Ereignis eingetreten ist.
$HOST_CONN_IP	IP-Adresse der Verbindung auf dem Geräts, auf dem das Ereignis eingetreten ist.

Beispiel:
Ausführbare Datei zur Benachrichtigung über Ereignisse (z. B. script1.bat), innerhalb der eine weitere ausführbare Datei (z. B. script2.bat) mit der Umgebungsvariable $COMPUTER gestartet wird. Beim Auftreten eines Ereignisses auf dem Gerät des Administrators wird die Datei script1.bat gestartet, die wiederum die Datei script2.bat mit der Umgebungsvariable $COMPUTER startet. Dadurch erhält der Administrator den Namen des Geräts, auf dem das Ereignis aufgetreten ist.

Kaspersky-Mitteilungen

In diesem Abschnitt wird beschrieben, wie Sie Kaspersky-Mitteilungen verwenden, konfigurieren und deaktivieren.

Über Kaspersky-Mitteilungen

Im Abschnitt mit den Kaspersky-Mitteilungen (**Überwachung → Mitteilungen von Kaspersky**) finden Sie Wissenswertes zu Ihrer Version von Kaspersky Security Center Linux und den verwalteten Anwendungen, die auf den verwalteten Geräten installiert sind. Kaspersky Security Center Linux aktualisiert die Informationen in diesem Abschnitt regelmäßig: Veraltete Mitteilungen werden entfernt und neue Informationen hinzugefügt.

Kaspersky Security Center Linux zeigt nur die Kaspersky-Mitteilungen an, die sich auf den derzeit verbundenen Administrationsserver und die auf dessen verwalteten Geräten installierten Kaspersky-Anwendungen beziehen. Die Mitteilungen werden für jeden Typ von Administrationsserver individuell angezeigt – primär, sekundär oder virtuell.

Der Administrationsserver benötigt eine Internetverbindung, um Kaspersky-Mitteilungen zu empfangen.

Die Mitteilungen enthalten Informationen der folgenden Typen:

- Sicherheitsrelevante Mitteilungen

  Mit sicherheitsrelevanten Mitteilungen werden die in Ihrem Netzwerk installierten Kaspersky-Anwendungen auf dem neuesten Stand und voll funktionsfähig gehalten. Die Mitteilungen können Informationen über kritische Updates für Kaspersky-Anwendungen, Korrekturen für gefundene Schwachstellen und Methoden zum Beheben sonstiger Probleme in Kaspersky-Anwendungen enthalten. Die sicherheitsrelevanten Mitteilungen sind standardmäßig aktiviert. Wenn Sie keine Mitteilungen erhalten möchten, können Sie diese Funktion deaktivieren.

  Um Ihnen die Informationen anzuzeigen, die Ihrer Netzwerkschutzkonfiguration entsprechen, sendet Kaspersky Security Center Linux Daten an die Kaspersky-Cloud-Server und empfängt nur die Mitteilungen, welche die in Ihrem Netzwerk installierten Kaspersky-Anwendungen betreffen. Der Datensatz, der an die Server gesendet werden kann, ist im Endbenutzer-Lizenzvertrag beschrieben, den Sie bei der Installation des Kaspersky Security Center Administrationsservers akzeptieren.

- Marketing-Mitteilungen

Marketing-Mitteilungen enthalten Informationen über Sonderangebote für Ihre Kaspersky-Anwendungen, Werbung und Neuigkeiten von Kaspersky. Marketing-Mitteilungen sind standardmäßig deaktiviert. Diese Art von Mitteilungen erhalten Sie nur, wenn Sie Kaspersky Security Network (KSN) aktiviert haben. Sie können Marketing-Mitteilungen deaktivieren, indem Sie KSN deaktivieren.

Um Ihnen nur relevante Informationen anzuzeigen, die für den Schutz Ihrer Netzwerkgeräte und für Ihren Aufgabenbereich hilfreich sein können, sendet Kaspersky Security Center Linux Daten an die Kaspersky-Cloud-Server und empfängt die entsprechenden Mitteilungen. Der Datensatz, der an die Server gesendet werden kann, wird im Abschnitt "Verarbeitete Daten" der KSN-Erklärung beschrieben.

Neue Informationen werden in Abhängigkeit ihrer Wichtigkeit in zwei Kategorien eingeteilt:

1. Kritische Information
2. Wichtige Neuigkeiten
3. Warnung
4. Information

Wenn im Abschnitt "Mitteilungen von Kaspersky" neue Informationen erscheinen, zeigt Kaspersky Security Center Web Console ein Benachrichtigungssymbol, welches der Ereigniskategorie der Mitteilungen entspricht. Sie können auf das Symbol klicken, um sich die Mitteilung im Abschnitt "Mitteilungen von Kaspersky" anzusehen.

Sie können die Einstellungen für Kaspersky-Mitteilungen konfigurieren, die Mitteilungskategorien wählen, die Sie ansehen möchten, und festlegen, wo das Benachrichtigungssymbol angezeigt werden soll. Wenn Sie keine Mitteilungen erhalten möchten, können Sie diese Funktion deaktivieren.

Einstellungen für die Kaspersky-Mitteilungen festlegen

Im Abschnitt Mitteilungen von Kaspersky können Sie die Einstellungen für Kaspersky-Mitteilungen konfigurieren, die Mitteilungskategorien wählen, die Sie ansehen möchten, und festlegen, wo das Benachrichtigungssymbol angezeigt werden soll.

So konfigurieren Sie die Mitteilungen von Kaspersky:

1. Gehen Sie im Hauptmenü zu **Überwachung** → **Mitteilungen von Kaspersky**.
2. Klicken Sie auf den Link **Einstellungen**.

   Das Fenster mit den Einstellungen für die Kaspersky-Mitteilungen wird geöffnet.
3. Geben Sie die folgenden Einstellungen an:

   - Wählen Sie die Ereigniskategorie der Mitteilungen, die Sie ansehen möchten. Die Mitteilungen anderer Kategorien werden nicht angezeigt.
   - Geben Sie an, wo das Benachrichtigungssymbol angezeigt werden soll. Das Symbol kann in allen Abschnitt der Konsole, sowie im Abschnitt **Überwachung** und in dessen Unterabschnitten angezeigt werden.
4. Klicken Sie auf die Schaltfläche **OK**.

   Die Einstellungen der Kaspersky-Mitteilungen sind angegeben.

Kaspersky-Mitteilungen deaktivieren

Im Abschnitt Mitteilungen von Kaspersky (**Überwachung → Mitteilungen von Kaspersky**) finden Sie Wissenswertes zu Ihrer Version von Kaspersky Security Center Linux und den verwalteten Anwendungen, die auf den verwalteten Geräten installiert sind. Wenn Sie keine Mitteilungen von Kaspersky erhalten möchten, können Sie diese Funktion deaktivieren.

Die Kaspersky-Mitteilungen enthalten zwei Arten von Informationen: sicherheitsrelevante Mitteilungen und Marketing-Mitteilungen. Sie können jeden Mitteilungstyp getrennt deaktivieren.

Um sicherheitsrelevante Mitteilungen zu deaktivieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.
   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Mitteilungen von Kaspersky** aus.
3. Stellen Sie die Umschaltfläche auf die Position **Sicherheitsrelevante Mitteilungen sind deaktiviert**.
4. Klicken Sie auf die Schaltfläche **Speichern**.
   Jetzt sind die Kaspersky-Mitteilungen deaktiviert.

Marketing-Mitteilungen sind standardmäßig deaktiviert. Marketing-Mitteilungen erhalten Sie nur, wenn Sie Kaspersky Security Network (KSN) aktiviert haben. Sie können diese Art von Mitteilungen deaktivieren, indem Sie KSN deaktivieren.

Um Marketing-Mitteilungen zu deaktivieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.
   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN-Proxy-Einstellungen** aus.
3. Deaktivieren Sie die Option **Kaspersky Security Network verwenden Aktiviert**.
4. Klicken Sie auf die Schaltfläche **Speichern**.
   Jetzt sind die Marketing-Mitteilungen deaktiviert.

Informationen über die Erkennung von Bedrohungen anzeigen

Sie können die Anzeige von Informationen über Alarme aktivieren oder deaktivieren.

*So aktivieren oder deaktivieren Sie die Anzeige von Abschnitt **Alarme** im Hauptmenü:*

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Einstellungen der Benutzeroberfläche**.
2. Aktivieren oder deaktivieren Sie die Option **Alarme von EDR anzeigen**.
3. Klicken Sie auf **Speichern**.

Wenn diese Option aktiviert ist, wird in der Konsole der Unterabschnitt **Alarme** im Abschnitt **Überwachung** des Hauptmenüs angezeigt. Im Unterabschnitt **Alarme** können Sie Informationen über die Erkennung von Bedrohungen auf den Endpunktgeräten anzeigen. Sie können auch ein Widget hinzufügen, das Informationen zu Alarmen anzeigt.

Damit detaillierte Informationen über erkannte Bedrohungen korrekt auf der Alarm-Karte angezeigt werden, müssen Sie das Plug-in für Kaspersky Endpoint Agent und die kompatible Version des Plug-ins für Kaspersky Endpoint Security installieren (Kaspersky Endpoint Security für Linux 12.1 oder höher, Kaspersky Endpoint Security for Mac 12.1 oder höher, oder Kaspersky Endpoint Security für Windows 12.6 oder höher).

Verwenden Sie das Menü **Filter**, um Benachrichtigungen nach Datum und Feldwerten zu filtern.

Das Feld **Objekttyp** enthält die folgenden Werte:

- unbekannt
- Phishing-Link
- Virus
- Trojaner
- Schädliches Programm
- Backdoor
- Wurm
- andere Anwendung
- Adware
- Pornware
- Gefährliches gepacktes Programm
- Gefährliches Verhalten

Das Feld **Automatische Antwort** enthält die folgenden Werte:

- Schädliches Objekt erkannt
- Objekt gelöscht
- Objekt desinfiziert
- Objekt konnte nicht desinfiziert werden

- Objekt in Quarantäne verschoben
- Kennwortgeschütztes Archiv gefunden
- Virus gefunden

Integrationen für die Reaktion auf Alarme

Wenn Sie über die Lizenz für Kaspersky Next XDR Optimum verfügen, können Sie Integrationen mit den folgenden Lösungen konfigurieren, um auf Bedrohungen zu reagieren:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Diese Integrationen sind verfügbar, wenn Sie den Administrationsserver unter einer Lizenz für Kaspersky Next XDR Optimum aktiviert haben.
Um Reaktionsmaßnahmen auszuführen, müssen Sie den Lizenzschlüssel für Kaspersky Next XDR Optimum für Ihre verwalteten Anwendungen bereitstellen.
Wenn Sie die Funktionen von Kaspersky Next XDR Optimum unter einer Demolizenz verwenden, müssen Sie zunächst einen sekundären physischen Administrationsserver hinzufügen, diesen sekundären Administrationsserver unter der Demolizenz aktivieren und anschließend den Lizenzschlüssel auf die Geräte verteilen, die von diesem Administrationsserver verwaltet werden.

Wenn Sie die Lizenz für Kaspersky Next EDR Optimum verwenden, müssen Sie die Anwendungen, die auf Ihren verwalteten Geräten installiert sind, nicht unter der Lizenz für Kaspersky Next XDR Optimum aktivieren. Sie müssen dies nur für neue Geräte tun (falls vorhanden).

Da die Lizenz von Kaspersky Next XDR Optimum Mandantenfähigkeit unterstützt, können Sie den Lizenzschlüssel zentral an verwaltete Anwendungen verteilen. Die automatische Verteilung der Lizenz auf sekundäre und virtuelle Administrationsserver wird nicht unterstützt.

Um die Integrationen zu konfigurieren, müssen Sie über die Berechtigungen **Lesen** und **Schreiben** für den Funktionsbereich **Allgemeine Funktionen: Anwendungsintegration** verfügen.

Integration mit Active Directory für die Ausführung von Reaktionsmaßnahmen konfigurieren

Die Integration mit Active Directory ermöglicht es Ihnen, Reaktionsmaßnahmen für Active Directory-Benutzer auszuführen, die vom Alarm betroffen oder daran beteiligt sind.

Um die Integration mit Active Directory für die Reaktion auf Alarme zu konfigurieren, müssen Sie den Kaspersky Security Center Linux Administrationsserver Version 15.4 oder höher verwenden.

Die Integration mit Active Directory für die Reaktion auf Alarme und die Einstellungen für die Untersuchung des Active Directory-Domänencontrollers (Adresse und Anmeldeinformationen des Domänencontrollers), die Sie bei der Konfiguration der Abfrage des Domänencontrollers angeben, sind zwei verschiedene Einstellungen. Da Sie sicherstellen müssen, dass der Benutzer, für den eine Reaktionsmaßnahme ausgeführt werden soll, über ein Active Directory-Konto verfügt, müssen Sie beide Integrationen konfigurieren: für die Untersuchung und für die Reaktion. Die Reihenfolge spielt dabei keine Rolle.

Die Integrationseinstellungen werden nicht vererbt und nur auf den Administrationsserver (physisch oder virtuell) angewendet, auf dem Sie diese Einstellungen konfigurieren.

Gehen Sie wie folgt vor, um die Integration mit Active Directory für die Reaktion auf Alarme zu konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie den Abschnitt **Verteilungspunkte** aus, klicken Sie auf den Namen des gewünschten Verteilungspunkts und wählen Sie anschließend im folgenden Eigenschaftenfenster den Abschnitt **Active Directory** aus.

   - Wählen Sie den Bereich **Active Directory-Antwort** aus.

3. Aktivieren Sie im rechten Bereich den Umschalter **Integration von Active Directory**.

   Wenn Sie die Integration später deaktivieren möchten, können Sie dies nur für alle Verbindungen tun, indem Sie den Umschalter **Integration von Active Directory** deaktivieren. Sie können die Integration nicht für eine einzelne Verbindung deaktivieren. Stattdessen können Sie die Verbindung löschen.

   > Wenn Sie den Umschalter **Integration von Active Directory** aktivieren oder deaktivieren, wird die Einstellung sowohl für den Abschnitt **Active Directory-Antwort** als auch für den Abschnitt **Verteilungspunkte** übernommen.

4. Stellen Sie eine Verbindung zum Active Directory-Domänencontroller her, indem Sie auf die Schaltfläche **Hinzufügen** klicken.

5. Passen Sie im nächsten Fenster die folgenden Parameter für die Verbindung an:

   - **Adresse des Domänencontrollers**

     Name des Computers, z. B. `server.mycompany.com`.

     Sie können mehrere Adressen angeben. Alle Domänencontroller, deren Adressen Sie angeben, müssen zu derselben Domäne gehören.

   - **Name der Active Directory-Domäne**

     Vollständig qualifizierter DNS-Domänenname, z. B. `mycompany.com`

     Sie können auch den SAM- oder NetBIOS-Namen angeben, z. B. `mycompany`

     Verwenden Sie Kleinbuchstaben. Wenn Sie mehrere Verbindungen für den Administrationsserver oder einen Verteilungspunkt erstellen, geben Sie für jede Verbindung einen anderen Namen an.

     > Um Reaktionsmaßnahmen durchzuführen, muss der in diesem Feld angegebene Active Directory-Domänenname mit dem im Alarm angegebenen Active Directory-Domänennamen übereinstimmen.

- **Anmelden**

  Benutzername des Active Directory-Kontos mit Administratorrechten, unter dem die Reaktionsmaßnahmen ausgeführt werden sollen.

- **Kennwort**

  Kennwort des Active Directory-Kontos mit Administratorrechten, unter dem die Reaktionsmaßnahmen ausgeführt werden sollen.

6. Wenn Sie den Verbindungsstatus überprüfen möchten, klicken Sie auf die Schaltfläche **Verbindung prüfen**.

   Wenn die Verbindung erfolgreich hergestellt wurde, wird der Status **Verbunden** angezeigt. Andernfalls lautet der Status **Fehlgeschlagen** und es wird eine Fehlermeldung für die Domänencontroller angezeigt, zu denen Sie keine Verbindung herstellen konnten.

> Sie müssen berücksichtigen, wie Sie eine Verbindung mit Active Directory herstellen: **von einem Linux-Gerät oder von einem Windows-Gerät**.

Verbindung von einem Linux-Gerät herstellen

Wenn Sie sich von einem Linux-Gerät aus mit einem Domänencontroller verbinden und sich bei ihm authentifizieren, sieht die Logik standardmäßig wie folgt aus:

1. Der Administrationsserver oder ein Verteilungspunkt versucht, über LDAPS eine Verbindung mit dem Domänencontroller herzustellen.

   Es wird eine strenge Überprüfung des LDAP-Serverzertifikats durchgeführt.

2. Um das Zertifikat zu validieren, legen Sie den öffentlichen Teil des Domänencontroller-Zertifikats im Zertifikatsspeicher des Systems ab.

   Für den Zugriff auf die Zertifikatskette wird der vom Betriebssystem abhängige Pfad zur Zertifizierungsstelle (CA) des Systems verwendet.

   Beispielsweise:

   - /etc/ssl/certs/ca-certificates.crt – Pfad für Debian-basierte Betriebssysteme (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem – Pfad für CentOS oder Red Hat.

3. Wenn die LDAP-Verbindung fehlschlägt, tritt ein Fehler auf und es wird kein anderes Verbindungsprotokoll verwendet.

> Bei Problemen mit LDAP können Sie sich an den Technischen Support von Kaspersky wenden.

Wenn Sie das Zertifikat nicht im Zertifikatsspeicher des Systems installieren möchten, können Sie das Flag KLNAG_LDAP_SSL_CACERT verwenden, um den Pfad zum Domänencontroller-Zertifikat festzulegen. Führen Sie dazu folgenden Befehl aus:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

wobei `</path/to/domain-controller/cert>` der Pfad zum öffentlichen Teil des Domänencontroller-Zertifikats ist.

Wenn der Pfad beispielsweise `"/var/opt/kaspersky/ldap_cert.crt"` lautet, lautet der Befehl `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Verbindung von einem Windows-Gerät herstellen

Wenn Sie sich von einem Windows-Gerät aus mit einem Domänencontroller verbinden und sich bei diesem authentifizieren, werden die Verbindungseinstellungen von der Domäne festgelegt.

Sie müssen nur Folgendes sicherstellen:

- LDAPS ist aktiviert und Port 636 ist auf dem Gerät verfügbar.
- Sie erlauben Verbindungen zum Domänencontroller durch eine Firewall oder einen Proxyserver.

7. Klicken Sie auf **Speichern**.

Das Fenster wird geschlossen und die Verbindung wird in der Verbindungstabelle angezeigt.

In der Verbindungstabelle sind folgende Aktionen möglich:

- Verbindungsparameter bearbeiten.

  Klicken Sie dazu für die gewünschte Verbindung auf den Link mit dem Parameter **Adresse des Domänencontrollers**. Ändern Sie im neuen Fenster die gewünschten Einstellungen und klicken Sie anschließend auf die Schaltfläche **Speichern**.

  Sie können nur die Parameter **Anmelden** und **Kennwort** bearbeiten.

- Verbindungen löschen.

  Aktivieren Sie dazu das Kontrollkästchen neben der Verbindung, die Sie löschen möchten, klicken Sie auf die Schaltfläche **Entfernen** in der Werkzeugleiste und bestätigen Sie anschließend das Löschen der Verbindung.

Integration mit der Kaspersky Automated Security Awareness Platform konfigurieren

Die Integration in die Kaspersky Automated Security Awareness Platform (im Folgenden auch KASAP genannt) ermöglicht die Zuordnung von KASAP-Lernkursen für Benutzer, die mit Alarmen verknüpft sind.

Die Integrationseinstellungen werden nicht vererbt und nur auf den Administrationsserver (physisch oder virtuell) angewendet, auf dem Sie diese Einstellungen konfigurieren.

Bevor Sie eine Integration in Kaspersky Security Center Web Console konfigurieren können, müssen Sie einen Autorisierungs-Token erstellen und eine URL für API-Anfragen in KASAP anfordern.

Gehen Sie wie folgt vor, um die Integration mit der Kaspersky Automated Security Awareness Platform zu konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wählen Sie den Abschnitt **KASAP** aus.

3. Aktivieren Sie im rechten Bereich den Umschalter **KASAP-Integration**.

4. Geben Sie die Einstellungen an, die für die Verbindung mit KASAP verwendet werden sollen:

   - **API-Token**: Token, das Sie für den Zugriff auf die Open API von KASAP erstellt haben.
   - **URL**: URL für API-Anfragen, die Sie beim Erstellen des API-Tokens erhalten haben.
   - **Proxyserver verwenden**: Umschalter, der die Verwendung eines Proxyservers für die Verbindung mit KASAP aktiviert.

     Der Umschalter ist standardmäßig deaktiviert.

5. Überprüfen Sie gegebenenfalls Ihre Einstellungen, indem Sie auf die Schaltfläche **Verbindung prüfen** klicken.

   Der Verbindungsstatus wird angezeigt.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Die Integration mit der Kaspersky Automated Security Awareness Platform ist konfiguriert.

Nachdem die Einstellungen der KASAP-Integration gespeichert wurden, können Sie die Liste der KASAP-Lerngruppen anzeigen, indem Sie auf die Schaltfläche **Gruppen anzeigen** klicken.

Wenn die Gruppenliste angezeigt wird, können Sie sie bei Bedarf aktualisieren, indem Sie auf die Schaltfläche **Gruppen aktualisieren** klicken.

Die Liste kann nach dem Öffnen nicht ausgeblendet werden. Wenn Sie den Umschalter für die **KASAP-Integration** deaktivieren, wird die Liste der KASAP-Gruppen nicht angezeigt.

Integration mit Kaspersky Threat Intelligence Portal Sandbox konfigurieren

Die Integration mit Kaspersky Threat Intelligence Portal (im Folgenden auch Kaspersky TIP genannt) ermöglicht die Ausführung der Dateien, die mithilfe von Kaspersky Sandbox in die **Quarantäne** verschoben wurden – eine sichere Umgebung, die von Ihrem Unternehmensnetzwerk isoliert ist.

Die Integrationseinstellungen werden nicht vererbt und nur auf den Administrationsserver (physisch oder virtuell) angewendet, auf dem Sie diese Einstellungen konfigurieren.

Bevor Sie die Integration konfigurieren, müssen Sie ein Autorisierungs-Token für API-Anfragen auf Kaspersky TIP anfordern.

Gehen Sie wie folgt vor, um die Integration mit Kaspersky TIP Sandbox zu konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wählen Sie **Kaspersky TIP** aus.

3. Aktivieren Sie im rechten Bereich den Umschalter **Integration**.

   Die Einstellungen für die Verbindung mit Kaspersky TIP werden angezeigt.

   > Wenn Sie nach dem Konfigurieren und Speichern der Integrationseinstellungen den Umschalter **Integration** deaktivieren, werden die Einstellungen nicht gelöscht, aber Sie können die Reaktionsmaßnahme nicht ausführen.

4. Klicken Sie auf die Schaltfläche **Token hinzufügen**, geben Sie im angezeigten Fenster das Token an, das Sie zuvor über Kaspersky TIP erhalten haben, und klicken Sie dann auf die Schaltfläche **Hinzufügen**.

   Das Fenster wird geschlossen und das API-Token wird hinzugefügt.

5. Wenn Sie für die Verbindung mit Kaspersky TIP einen Proxyserver verwenden möchten, aktivieren Sie den Umschalter **Proxyserver verwenden**.

   Der Umschalter ist standardmäßig deaktiviert.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Die Integration mit Kaspersky TIP Sandbox ist konfiguriert.

Jetzt können Sie Dateien aus der **Quarantäne** zur Bedrohungsanalyse an Kaspersky TIP Sandbox senden. Die maximale Größe einer Datei beträgt 100 MB.

Da die Lizenz für Kaspersky Next XDR Optimum die Mandantenfähigkeit unterstützt, können Dateien, die in die **Quarantäne** verschoben werden, nach Mandanten aufgeteilt werden. Diese Trennung auf Mandantenebene kann auch für das Senden von Dateien an Kaspersky TIP Sandbox und die Anzeige der Ergebnisse angewendet werden, wenn der Administrator ein dediziertes TIP-Konto und ein API-Token für jeden Mandanten verwendet. Eine zentrale Verwaltung des Abschnitts **Quarantäne** für alle Mandanten ist jedoch nicht möglich, da die Quarantäneliste Objekte nicht entsprechend der Serverhierarchie anzeigt.

Alarme nach Attributen gruppieren

Die Aggregation von Alarmen hilft bei der Identifizierung von Alarmen, die sich auf denselben Vorfall beziehen können, und vereinfacht so den Untersuchungsprozess.

Um die Funktionalität der Alarm-Aggregation zu aktivieren, müssen Sie Folgendes tun:

- Aktivieren Sie im Hauptmenü den Unterabschnitt **Alarme**.
- Aktivieren Sie den Administrationsserver unter einer Lizenz für Kaspersky Next XDR Optimum und stellen Sie anschließend den Lizenzschlüssel für Kaspersky Next XDR Optimum für Ihre verwalteten Anwendungen bereit.

  Wenn Sie Kaspersky Next XDR Optimum unter einer Demolizenz verwenden, müssen Sie zuerst einen sekundären physischen Administrationsserver hinzufügen und den Server anschließend unter dieser Lizenz aktivieren.

Wenn Sie die Lizenz für Kaspersky Next EDR Optimum verwenden, müssen Sie die Anwendungen, die auf Ihren verwalteten Geräten installiert sind, nicht unter der Lizenz für Kaspersky Next XDR Optimum aktivieren. Sie müssen dies nur für neue Geräte tun, falls vorhanden.
Da die Lizenz für Kaspersky Next XDR Optimum die Mandantenfähigkeit unterstützt, können Sie den Lizenzschlüssel zentral an verwaltete Anwendungen verteilen. Die automatische Verteilung der Lizenz auf sekundäre und virtuelle Administrationsserver wird nicht unterstützt.

Sie können Alarme nach Gerätename, Konto oder Hash-Name (SHA256) aggregieren.

Alarme werden nur dann nach einem Attribut aggregiert, wenn dieses Attribut nicht leer ist.

Alarme werden aggregiert, wenn sie mindestens ein Attribut gemeinsam haben und innerhalb von 24 Stunden nach einem anderen Alarm in der Gruppe auftreten.

Gehen Sie wie folgt vor, um Alarme nach Attributen zu aggregieren:

1. Gehen Sie im Hauptmenü zu **Überwachung** → **Alarme**.
2. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie den Umschalter **Aggregation von Alarmen** und wählen Sie dann ein oder mehrere Attribute aus, nach denen Alarme aggregiert werden sollen:
     - **Gerätename**
     - **Benutzerkonto**
     - **Datei-Hash (SHA256)**

     Die Attribute **Gerätename** und **Benutzerkonto** sind standardmäßig ausgewählt.
   - Klicken Sie auf das Einstellungen-Symbol (⚙). Gehen Sie im nächsten Fenster **Tabelleneinstellungen** zur Registerkarte **Gruppierung**. Wählen Sie **ID der Aggregationsgruppe** aus und klicken Sie auf **Übernehmen**.

   Wenn das Aggregieren aktiviert ist, werden die Alarme nach **Ereigniszeitpunkt** vom neuesten zum ältesten sortiert. Zusätzliche Sortieroptionen werden nicht unterstützt. Wenn Sie eine andere Optionsgruppe auswählen, wird das Aggregieren deaktiviert.

In der Tabelle werden die nach Attributen aggregierten Alarme angezeigt. Nicht aggregierte Alarme werden unten in der Tabelle angezeigt.

Jeder Alarm wird nach dem Aggregieren nur einer Gruppe zugewiesen.

Cloud Discovery

Mit Kaspersky Security Center Linux können Sie die Verwendung von Cloud-Diensten auf verwalteten Windows-Geräten überwachen und den Zugriff auf unerwünschte Cloud-Dienste blockieren. Cloud Discovery überwacht die Zugriffsversuche von Benutzern auf diese Dienste sowohl über Browser als auch über Desktop-Anwendungen. Es überwacht zusätzlich die Versuche von Benutzern, über unverschlüsselte Verbindungen (z. B. mithilfe des HTTP-Protokolls) auf Cloud-Dienste zuzugreifen. Diese Funktion hilft Ihnen, die heimliche und unbefugte Verwendung von Cloud-Diensten zu erkennen und zu stoppen.

Die Funktion zum Blockieren ist nur verfügbar, wenn Sie Kaspersky Security Center Linux unter einer Lizenz für Kaspersky Next EDR Optimum oder Kaspersky Next XDR Expert aktiviert haben.

Die Funktion zum Blockieren ist nur verfügbar, wenn Sie Kaspersky Endpoint Security 11.2 für Windows oder höher verwenden. Ältere Versionen der Sicherheitsanwendung erlauben Ihnen lediglich die Überwachung der Verwendung von Cloud-Diensten.

Sie können die Cloud Discovery-Funktion aktivieren und die Sicherheitsrichtlinien oder Profile auswählen, für die Sie die Funktion aktivieren möchten. Sie können die Funktion auch separat in jeder Sicherheitsrichtlinie oder jedem Profil aktivieren oder deaktivieren. Sie können den Zugriff auf Cloud-Dienste blockieren, auf welche die Benutzer nicht zugreifen dürfen.

Damit Sie den Zugriff auf unerwünschte Cloud-Dienste blockieren können, müssen die folgenden Voraussetzungen erfüllt sein:

- Sie verwenden Kaspersky Endpoint Security 11.2 für Windows oder höher. Ältere Versionen der Sicherheitsanwendung erlauben Ihnen lediglich die Überwachung der Verwendung von Cloud-Diensten.
- Sie haben eine Lizenz der Stufe "Kaspersky Next" erworben, in deren Rahmen Sie den Zugriff auf unerwünschte Cloud-Dienste blockieren können. Weitere Informationen finden Sie in der Hilfe zu Kaspersky Next.

Das Cloud Discovery-Widget und die Berichte von Cloud Discovery enthalten Informationen über erfolgreiche und blockierte Zugriffsversuche auf Cloud-Dienste. Das Widget zeigt auch für jeden Cloud-Dienst die Risikostufe an. Kaspersky Security Center Linux ruft die Informationen zur Verwendung von Cloud-Diensten von allen verwalteten Geräten ab, die nur durch jene Sicherheitsrichtlinien oder Sicherheitsprofile geschützt sind, für welche die Funktion aktiviert ist.

Cloud Discovery über das Widget aktivieren

Die Cloud Discovery-Funktion ruft die Informationen zur Verwendung von Cloud-Diensten von allen verwalteten Geräten ab, die nur durch jene Sicherheitsrichtlinien geschützt sind, für welche die Funktion aktiviert ist. Sie können Cloud Discovery nur für die Richtlinie von Kaspersky Endpoint Security für Windows aktivieren oder deaktivieren.

Es gibt zwei Möglichkeiten, die Cloud Discovery-Funktion zu aktivieren:

- Mithilfe des Cloud Discovery-Widgets.
- In den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows.

  Weitere Informationen zur Aktivierung von Cloud Discovery in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows im Abschnitt Cloud Discovery.

Beachten Sie, dass Sie Cloud Discovery nur in den Richtlinienparametern von Kaspersky Endpoint Security für Windows deaktivieren können.

Um Cloud Discovery zu aktivieren, müssen Sie für den Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen** über die Berechtigung **Schreiben** verfügen.

So aktivieren Sie die Cloud Discovery-Funktion mithilfe des Cloud Discovery-Widgets:

1. Wechseln Sie zu Kaspersky Security Center Linux.
2. Gehen Sie im Hauptmenü zu **Überwachung** → **Dashboard**.
3. Klicken Sie im Widget **Cloud Discovery** auf **Aktivieren**.

   Wenn Sie Kaspersky Endpoint Security für Windows Version 12.4 installiert haben, aktivieren Sie Cloud Discovery in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows. Weitere Informationen finden Sie im Abschnitt Cloud Discovery der Hilfe zu Kaspersky Endpoint Security für Windows.

   Wenn Sie Kaspersky Endpoint Security für Windows bis Version 12.4 verwenden, aktualisieren Sie das Plug-in für Kaspersky Endpoint Security für Windows auf Version 12.5.

4. Wählen Sie im folgenden Fenster **Cloud Discovery aktivieren** die Sicherheitsrichtlinien aus, für welche Sie die Funktion aktivieren möchten, und klicken Sie anschließend auf **Aktivieren**.

   Die folgenden Richtlinieneinstellungen werden automatisch aktiviert: **Skript zum Interagieren mit Webseiten in den Web-Datenverkehr einbinden**, **Überwachen von Web-Sitzungen** und **Untersuchung verschlüsselter Verbindungen**.

Die Cloud Discovery-Funktion ist aktiviert und das Widget wurde dem Dashboard hinzugefügt.

Das Cloud Discovery-Widget zum Dashboard hinzufügen

Sie können das **Cloud Discovery-Widget** zum Dashboard hinzufügen, um die Nutzung von Cloud-Diensten auf verwalteten Geräten zu überwachen.

Um das Cloud Discovery-Widget zum Dashboard hinzuzufügen, müssen Sie das Recht **Schreiben** für den Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen** haben.

So fügen Sie das Cloud Discovery-Widget zum Dashboard hinzu:

1. Gehen Sie zu Kaspersky Security Center Linux.
2. Gehen Sie im Hauptmenü zu **Überwachung** → **Dashboard**.
3. Klicken Sie auf **Widget hinzufügen oder wiederherstellen**.
4. Klicken Sie in der Liste der verfügbaren Widgets auf das Chevron-Symbol (›) neben der Kategorie **Andere**.
5. Wählen Sie das Widget **Cloud Discovery** aus und klicken Sie anschließend auf **Hinzufügen**.

   Wenn die Cloud Discovery-Funktion deaktiviert ist, befolgen Sie die Anweisungen im Abschnitt "Cloud Discovery über das Widget aktivieren".

Das ausgewählte Widget wird am Ende des Dashboards hinzugefügt.

Informationen zur Nutzung von Cloud-Diensten anzeigen

Sie können das **Cloud Discovery-Widget** anzeigen, das Informationen zu versuchten Zugriffen auf Cloud-Dienste zur Verfügung stellt. Außerdem zeigt das Widget für jeden Cloud-Dienst die Risikostufe an.
Kaspersky Security Center Linux ruft die Informationen zur Verwendung von Cloud-Diensten von allen verwalteten Geräten ab, die nur durch jene Sicherheitsprofile geschützt sind, für welche die Funktion aktiviert ist.

Stellen Sie vor dem Betrachten sicher, dass die folgenden Bedingungen erfüllt sind:

- Das Cloud Discovery-Widget wurde zum Dashboard hinzugefügt.
- Die Cloud Discovery-Funktion ist aktiviert.
- Sie verfügen über die Berechtigung **Lesen** für den Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen**.

So zeigen Sie das Cloud Discovery-Widget an:

1. Gehen Sie zu Kaspersky Security Center Linux.
2. Gehen Sie im Hauptmenü zu **Überwachung** → **Dashboard**.

   Das **Cloud Discovery** wird auf dem Dashboard angezeigt.
3. Wählen Sie auf der linken Seite des Widgets **Cloud Discovery** eine Kategorie für Cloud-Dienste aus.

   In der Tabelle auf der rechten Seite des Widgets werden für die ausgewählte Kategorie bis zu fünf Dienste angezeigt, auf welche die Benutzer am häufigsten versuchen zuzugreifen. Es werden sowohl erfolgreiche als auch blockierte Versuche gezählt.
4. Wählen Sie auf der rechten Seite des Widgets einen bestimmten Dienst aus.

   Die untere Tabelle enthält bis zu zehn Geräte, die am häufigsten versuchen, auf den Dienst zuzugreifen. In dieser Tabelle können Sie zwei Arten von Berichten erstellen: Bericht über erfolgreiche Zugriffsversuche und Bericht über blockierte Zugriffsversuche.

   Darüber hinaus können Sie in dieser Tabelle den Zugriff auf die Cloud-Dienste für Reihe von Geräten.

Das Widget zeigt die angeforderten Informationen an.

Im angezeigten Widget können Sie:

- Zum Abschnitt **Überwachung** → **Berichte** wechseln, um die Berichte von Cloud Discovery anzuzeigen.
- Den Zugriff auf den ausgewählten Cloud-Dienst blockieren oder erlauben.

Die Funktion zum Blockieren ist nur verfügbar, wenn Sie Kaspersky Security Center Linux unter einer Lizenz für Kaspersky Next EDR Optimum oder Kaspersky Next XDR Expert aktiviert haben.

Die Funktion zum Blockieren ist nur verfügbar, wenn Sie Kaspersky Endpoint Security 11.2 für Windows oder höher verwenden. Ältere Versionen der Sicherheitsanwendung erlauben Ihnen lediglich die Überwachung der Verwendung von Cloud-Diensten.

Risikostufe eines Cloud-Dienstes

Cloud Discovery gibt für jeden Cloud-Dienst eine Risikostufe an. Anhand der Risikostufe können Sie Cloud-Dienste identifizieren, die nicht den Sicherheitsanforderungen Ihres Unternehmens entsprechen. Bei der Entscheidung, ob der Zugriff auf einen bestimmten Dienst blockiert werden muss, können Sie beispielsweise die Risikostufe des Dienstes berücksichtigen.

Die Risikostufe ist ein geschätzter Index, der weder etwas über die Qualität eines Cloud-Dienstes, noch über den Dienstanbieter aussagt. Die Risikostufe stellt lediglich eine Empfehlung von Kaspersky-Experten dar.

Die Risikostufen der Cloud-Dienste werden im Cloud Discovery-Widget und in der Liste aller überwachten Cloud-Dienste angezeigt.

Zugriffs auf unerwünschte Cloud-Dienste blockieren

Sie können den Zugriff auf Cloud-Dienste blockieren, auf welche die Benutzer nicht zugreifen sollen. Gleichermaßen können Sie den Zugriff auf zuvor gesperrte Cloud-Dienste erlauben.

Bei der Entscheidung, ob der Zugriff auf einen bestimmten Dienst blockiert werden soll, können Sie unter anderem die Risikostufe des Dienstes berücksichtigen.

Sie können den Zugriff auf Cloud-Dienste für eine Sicherheitsrichtlinie oder ein Profil blockieren oder erlauben.

Es gibt zwei Möglichkeiten, den Zugriff auf unerwünschte Cloud-Dienste zu blockieren:

- Mithilfe des Widgets von Cloud Discovery.

  In diesem Fall können Sie den Zugriff auf die Dienste einzeln sperren.

- In den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows.

  In diesem Fall können Sie den Zugriff auf die Dienste einzeln oder gleich für eine ganze Kategorie blockieren.

  Weitere Informationen zur Aktivierung von Cloud Discovery in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows im Abschnitt Cloud Discovery.

So blockieren oder erlauben Sie den Zugriff auf einen Cloud-Dienst mithilfe des Widgets:

1. Öffnen Sie das Cloud Discovery-Widget und wählen Sie anschließend den erforderlichen Cloud-Dienst aus.
2. Suchen Sie im Bereich **Top 10 der Geräte, die diesen Dienst verwenden** nach der Sicherheitsrichtlinie oder dem Profil, für die bzw. das Sie den Dienst blockieren oder zulassen möchten.
3. Führen Sie in der entsprechenden Zeile in der Spalte **Zugriffsstatus in Richtlinie oder Profil** einen der folgenden Schritte aus:
   - Um den Dienst zu blockieren, wählen Sie in der Dropdown-Liste die Option **Blockiert** aus.
   - Um den Dienst zu erlauben, wählen Sie in der Dropdown-Liste die Option **Zugelassen** aus.
4. Klicken Sie auf **Speichern**.

Der Zugriff auf den ausgewählten Dienst wird für die Sicherheitsrichtlinie oder das Profil gesperrt oder erlaubt.

Ereignisse in SIEM-Systeme exportieren

Dieser Abschnitt beschreibt, wie Sie den Export von Ereignissen in ein SIEM-System konfigurieren.

Ereignisexport in SIEM-Systeme konfigurieren

Mit Kaspersky Security Center Linux können Sie den Export von Ereignissen in SIEM-Systeme mit einer der folgenden Methoden konfigurieren: Export in ein beliebiges SIEM-System im Syslog-Format, Export in die SIEM-Systeme von QRadar, Splunk und ArcSight im LEEF- und CEF-Format sowie direkter Export in SIEM-Systeme aus der Ereignisdatenbank von Kaspersky Security Center. Nach Abschluss dieses Szenarios sendet der Administrationsserver automatisch Ereignisse an ein SIEM-System.

Erforderliche Vorrausetzungen

Bevor Sie mit der Konfiguration des Ereignisexports in Kaspersky Security Center Linux beginnen:

- Weitere Informationen über die Exportmethoden.
- Stellen Sie sicher, dass Sie die Werte der Systemeinstellungen kennen.

> Sie können die Schritte in diesem Szenario in beliebiger Reihenfolge ausführen.

Der Vorgang des Ereignisexports in ein SIEM-System umfasst die folgenden Schritte:

- **Konfigurieren des SIEM-Systems, sodass es Ereignisse aus Kaspersky Security Center Linux empfängt**

  Anleitung: Einstellungen für den Ereignisexport in das SIEM-System

- **Auswählen der Ereignisse, die Sie in das SIEM-System exportieren möchten**

  Markieren der Ereignisse, die Sie in das SIEM-System exportieren möchten. Markieren Sie zuerst die allgemeinen Ereignisse, die in allen verwalteten Kaspersky-Anwendungen auftreten. Dann können Sie die Ereignisse für bestimmte verwaltete Kaspersky-Anwendungen markieren.

- **Konfigurieren des Exports von Ereignissen in das SIEM-System**

  Der Export von Ereignissen kann auf folgende Weisen erfolgen:

  - Mittels der Protokolle TCP, UDP oder TLS over TCP
  - Mittels direktem Ereignisexport aus der Datenbank von Kaspersky Security Center (In der Datenbank von Kaspersky Security Center ist eine Auswahl an öffentlichen Ansichten verfügbar. Die Beschreibung dieser Ansichten finden Sie im Dokument klakdb.chm).

Ergebnisse

Nach der Konfiguration des Ereignisexports in ein SIEM-System, können Sie sich die Exportergebnisse ansehen, wenn Sie zu exportierende Ereignisse ausgewählt haben.

Vorläufige Bedingungen

Wenn Sie den automatischen Ereignisexport in Kaspersky Security Center Linux einrichten, müssen Sie einige Einstellungen des SIEM-Systems angeben. Es ist empfehlenswert, diese Einstellungen im Voraus zu bestimmen, damit die Einstellungen für Kaspersky Security Center Linux vorbereitet werden können.

Für die Einstellungen des automatischen Ereignisexports ins SIEM-System müssen die Werte der folgenden Einstellungen bekannt sein:

- **Serveradresse des SIEM-Systems**

  IP-Adresse des Servers, auf dem das verwendete SIEM-System installiert ist. Dieser Wert muss in den Einstellungen des SIEM-Systems genau bestimmt werden.

- **Serverport des SIEM-Systems**

  Port, über den eine Verbindung zwischen Kaspersky Security Center Linux und dem Server des SIEM-Systems hergestellt wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center Linux und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

- **Protokoll**

  Das Protokoll, das für die Übertragung von Daten aus Kaspersky Security Center Linux ins SIEM-System verwendet wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center Linux und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

Über den Ereignisexport

Kaspersky Security Center Linux ermöglicht das automatische Empfangen von Informationen über Ereignisse, die während der Ausführung des Administrationsservers und auf verwalteten Geräten installierter Kaspersky-Anwendungen aufgetreten sind. Die Informationen über Ereignisse werden in der Administrationsserver-Datenbank gespeichert.

Sie können den Ereignisexport innerhalb zentralisierten Systemen verwenden, die sich mit Fragen der Sicherheit auf organisatorischer und technischer Ebene und der Überwachung des Sicherheitssystems beschäftigen sowie Daten aus verschiedenen Lösungen konsolidieren. Dazu gehören SIEM-Systeme, die eine Analyse der Warnungen der Sicherheitssysteme und Ereignisse der Netzwerkhardware und Anwendungen im Echtzeitbetrieb gewährleisten, sowie Security Operation Center (SOC).

Diese Systeme erhalten Daten aus vielen Quellen, einschließlich Netzwerke, Sicherheitssysteme, Server, Datenbanken und Anwendungen. Ferner gewährleisten SIEM-Systeme eine Zusammenfassung der bearbeiteten Daten, damit Sie keine kritischen Ereignisse überspringen können. Außerdem führen diese Systeme eine automatische Analyse der verbundenen Ereignisse und der Alarme zur Benachrichtigung der Administratoren über Fragen des Sicherheitssystems, die eine sofortige Entscheidung fordern, durch. Die Benachrichtigungen können im Indikatorbereich angezeigt oder über dritte Kanäle, beispielsweise E-Mail, versendet werden.

Am Ablauf des Ereignisexports aus Kaspersky Security Center Linux in externe SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse (Kaspersky Security Center Linux) und der Empfänger der Ereignisse (ein SIEM-System). Für einen erfolgreichen Ereignisexport müssen die Einstellungen sowohl im verwendeten SIEM-System als auch in Kaspersky Security Center Linux angepasst werden. Die Reihenfolge der Einstellungen hat keine Bedeutung: Sie können entweder zuerst den Versand der Ereignisse in Kaspersky Security Center Linux und dann das Empfangen der Ereignisse im SIEM-System anpassen oder umgekehrt.

Methoden für den Versand von Ereignissen aus Kaspersky Security Center Linux

Es gibt drei Methoden für den Versand von Ereignissen aus Kaspersky Security Center Linux in die externen Systeme:

- Versand von Ereignissen gemäß dem Protokoll Syslog in ein beliebiges SIEM-System

  Gemäß dem Protokoll Syslog können beliebige Ereignisse, die auf dem Kaspersky Security Center Administrationsserver und in den auf den verwalteten Geräten installierten Kaspersky-Anwendungen auftreten, übertragen werden. Das Syslog-Protokoll ist ein Standardprotokoll für das Aufzeichnen von Nachrichten. Sie können es für den Export von Ereignissen ein beliebiges SIEM-System verwenden.

  Zu diesem Zweck müssen Sie die Ereignisse markieren, die Sie an das SIEM-System weiterleiten möchten. Die Ereignisse können Sie in Kaspersky Security Center Web Console markieren. Es werden nur markierte Ereignisse an das SIEM-System weitergeleitet. Wenn Sie nichts markiert haben, werden keine Ereignisse weitergeleitet.

- Versand von Ereignissen gemäß den Protokollen CEF und LEEF in die Systeme QRadar, Splunk und ArcSight

  Sie können die Protokolle CEF und LEEF verwenden, um allgemeine Ereignisse zu exportieren. Die Protokolle CEF und LEEF sind im Gegensatz zum Protokoll Syslog nicht universell. Stattdessen werden alle allgemeinen Ereignisse exportiert. Um Ereignisse von Kaspersky Security Center Linux in Ereignisse im CEF- und LEEF-Format zu konvertieren, können Sie die Datei siem_conversion_rules.xml verwenden. Diese Datei enthält die Liste der Ereignisattribute von Kaspersky Security Center Linux und deren entsprechenden Ereignisattribute im CEF- und LEEF-Format. Zusätzlich enthält die Datei "siem_conversion_rules.xml" Regeln zum Generieren von Nachrichten zu den entsprechenden Ereignissen. Diese Datei ist im Lieferumfang von Kaspersky Security Center Linux enthalten.

Anders als das Syslog-Protokoll sind das CEF- und das LEEF-Protokoll nicht universell. CEF und LEEF sind für die entsprechenden SIEM-Systeme (QRadar, Splunk und ArcSight) vorgesehen. Wenn Sie daher Ereignisse über eines dieser Protokolle exportieren, verwenden Sie den erforderlichen Parser im SIEM-System.

- Direkt aus der Datenbank von Kaspersky Security Center Linux in ein beliebiges SIEM-System

  Diese Methode für den Ereignisexport kann für das Empfangen von Ereignissen direkt aus den öffentlichen Ansichten der Datenbank mithilfe von SQL-Abfragen verwendet werden. Die Ausführungsergebnisse der Anfrage werden in einer xml-Datei gespeichert und können als Eingangsdaten für das externe System verwendet werden. Nur Ereignisse, die in öffentlichen Ansichten verfügbar sind, können direkt aus der Datenbank exportiert werden.

Empfangen von Ereignissen im SIEM-System

Das SIEM-System muss die von Kaspersky Security Center Linux übertragenen Ereignisse übernehmen und korrekt analysieren. Dazu müssen die Einstellungen des SIEM-Systems angepasst werden. Die Konfiguration hängt vom verwendeten speziellen SIEM-System ab. Es gibt jedoch eine Anzahl von allgemeinen Schritten in der Konfiguration aller SIEM-Systeme, etwa die Konfiguration des Empfängers und des Parsers.

Über das Konfigurieren des Ereignisexports in ein SIEM-System

Am Ablauf des Ereignisexports aus Kaspersky Security Center Linux in externe SIEM-Systeme sind zwei Seiten beteiligt: der Absender der Ereignisse (Kaspersky Security Center Linux) und der Empfänger der Ereignisse (ein SIEM-System). Sie müssen den Ereignisexport im verwendeten SIEM-System und in Kaspersky Security Center Linux anpassen.

Die Einstellungen, die im SIEM-System vorgenommen werden, sind vom System abhängig, das Sie verwenden. Im Allgemeinen müssen für alle SIEM-Systeme der Empfänger der Nachrichten und, falls erforderlich, der Nachrichtenparser angepasst werden, damit die erhaltenen Nachrichten auf die Felder verteilt werden können.

Einstellungen des Empfängers der Nachrichten

Für das SIEM-Systems muss der Empfänger für den Erhalt der Ereignisse, die von Kaspersky Security Center Linux gesendet werden, angepasst werden. Im Allgemeinen müssen im SIEM-System die folgenden Einstellungen angegeben werden:

- **Exportprotokoll**

  Ein Protokoll zum Übertragen von Nachrichten, entweder UDP, TCP oder TLS over TCP. Es muss dasselbe Protokoll angegeben werden wie in Kaspersky Security Center Linux.

- **Port**

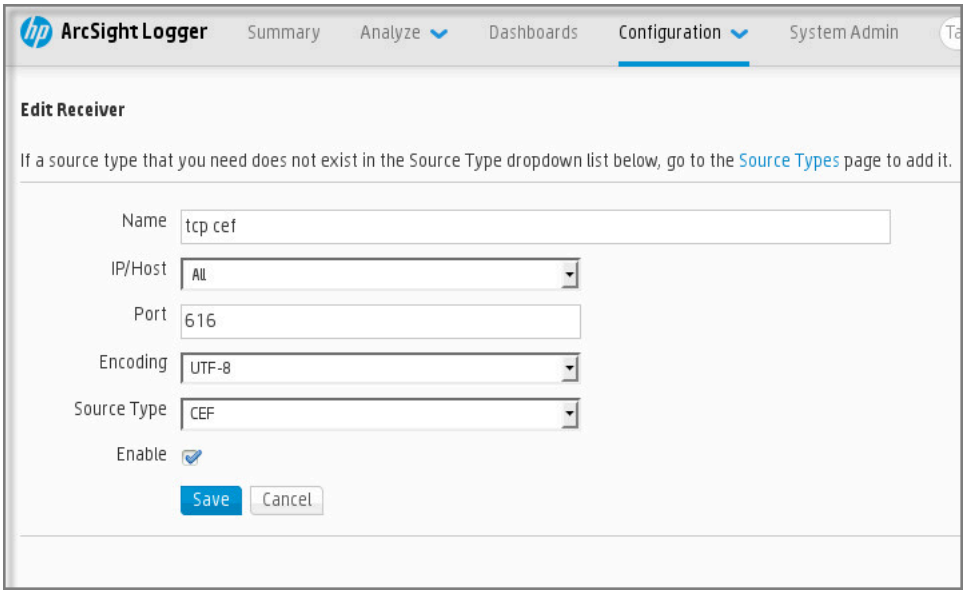
  Geben Sie die Portnummer für die Verbindung mit Kaspersky Security Center Linux an. Dieser Port muss derselbe sein wie der Port, den Sie in Kaspersky Security Center Linux bei der Konfiguration für das SIEM-System angeben.

- **Datenformat**

  Geben Sie das Syslog-, CEF- oder LEEF-Format an.

Je nachdem, welches SIEM-System Sie verwendetem, kann es erforderlich sein, erweiterte Einstellungen für den Empfänger der Nachrichten anzugeben.

Auf der unteren Abbildung dienen die Einstellungen des Empfängers in ArcSight als Beispiel.



Einstellungen des Empfängers in ArcSight

Nachrichtenparser

Die exportierten Ereignisse werden in Form von Nachrichten an das SIEM-System übergeben. Dann wird für diese Nachrichten der Parser verwendet, damit die Informationen über die Ereignisse entsprechend ins SIEM-System übergeben werden. Die Nachrichtenparser sind im SIEM-System integriert und werden für die Aufteilung der Nachrichten in Felder wie Nachrichten-ID, Signifikanz, Beschreibung und Parameter verwendet. Dadurch hat das SIEM-System die Möglichkeit, die Ereignisse, die aus Kaspersky Security Center Linux empfangen werden, so zu verarbeiten, dass sie in der Datenbank des SIEM-Systems gespeichert werden.

Über das Exportieren von Ereignissen mittels der Formate CEF und LEEF

Die CEF- und LEEF-Formate können verwendet werden, um allgemeine Ereignisse, Ereignisse über Änderungen von Richtlinien und Ereignisse, die von Kaspersky-Anwendungen an den Administrationsserver übertragen werden, in SIEM-Systeme zu exportieren. Der Satz der zu exportierenden Ereignisse ist vordefiniert, es gibt keine Möglichkeit, die zu exportierenden Ereignisse auszuwählen. Bevor Ereignisse aus Kaspersky Security Center Linux an ein SIEM-System (QRadar, ArcSight oder Splunk) übertragen werden können, müssen diese Ereignisse in das CEF- oder LEEF-Format konvertiert werden. Dies geschieht unter Verwendung der Regeln, die in der Datei "siem_conversion_rules.xml" enthalten sind.

Das Exportformat kann abhängig vom verwendeten SIEM-System ausgewählt werden. In der folgenden Tabelle sind die SIEM-Systeme und die ihnen entsprechenden Exportformate angeführt.

SIEM-System	Exportformat
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) ist ein spezielles Format für Ereignisprotokollierung in IBM Security QRadar SIEM. QRadar kann Ereignisse, die gemäß dem LEEF-Protokoll übergeben werden, sammeln, identifizieren und bearbeiten. Für das LEEF-Protokoll muss die UTF-8-Kodierung verwendet werden. Ausführlicheren Informationen über das LEEF-Protokoll finden Sie im IBM Knowledge Center.

- CEF ist ein Standard der Verwaltung vom Typ "offenes Protokoll", der die Kompatibilität der Informationen des Sicherheitssystems verschiedener Netzwerkgeräte und Apps verbessert. Das CEF-Protokoll ermöglicht die Verwendung eines allgemeinen Formats für das Ereignisprotokoll, damit die Managementsysteme für Unternehmen die Daten für die Analyse problemlos abrufen und zusammenfassen können. Für das CEF-Protokoll muss die UTF-8-Kodierung verwendet werden.

Automatischer Export bedeutet, dass Kaspersky Security Center Linux die allgemeinen Ereignisse ins SIEM-System sendet. Der automatische Export der Ereignisse beginnt sofort nach der Aktivierung. In diesem Abschnitt ist der Ablauf zur Aktivierung des automatischen Exports von Ereignissen beschrieben.

Ereignisse in das CEF- oder LEEF-Format konvertieren

Bevor Ereignisse aus Kaspersky Security Center an ein SIEM-System (QRadar, ArcSight oder Splunk) übertragen werden können, müssen diese Ereignisse in das CEF- oder LEEF-Format konvertiert werden. Dies geschieht unter Verwendung der Regeln, die in der Datei "siem_conversion_rules.xml" enthalten sind. Diese Datei ist im Lieferumfang von Kaspersky Security Center Linux enthalten.

Die Datei "siem_conversion_rules.xml" enthält die vordefinierten Interpretationsregeln zum Konvertieren von Ereignissen in das CEF- und LEEF-Format. Wenn Sie zusätzliche Regeln für die Ereignisinterpretation verwenden möchten, können Sie diese der Datei manuell hinzufügen.

Die Datei "siem_conversion_rules.xml" enthält die folgenden Abschnitte:

- `<product name="SP_QRADAR" vendor="IBM">`

  Dieser Abschnitt enthält Regeln zum Erstellen von Ereignissen im LEEF-Format, die in ein SIEM-System von QRadar exportiert werden können.

- [[<product name="SP_ARCSIGHT" vendor="HP">]]

  Dieser Abschnitt enthält Regeln zum Erstellen von Ereignissen im CEF-Format, die in SIEM-Systeme von ArcSight oder Splunk exportiert werden können.

- `<product name="Kaspersky SIEM" vendor="Kaspersky">`.

  Dieser Abschnitt enthält Regeln zum Erstellen von Ereignissen im CEF-Format, die nach KUMA exportiert werden können.

Jeder Abschnitt besitzt den Unterabschnitt `<common>`, in dem sich die Ereignisattribute von Kaspersky Security Center Linux und deren entsprechenden Ereignisattribute im LEEF-Format befinden. Diese gemeinsamen Attribute werden für alle Arten von Ereignissen verwendet, die exportiert werden können.

Zusätzlich besitzt jeder Abschnitt den Unterabschnitt `<event>`. Jeder `<event>`-Unterabschnitt enthält weitere Attribute, die den Attributen des Abschnitts `<common>` hinzugefügt werden.

Sie können der Datei "siem_conversion_rules.xml" eine neue Regel zur Ereignisgenerierung manuell hinzufügen.

So fügen Sie eine neue Regel zur Ereignisgenerierung hinzu:

1. Fügen Sie dem Abschnitt `<product name="SP_QRADAR" vendor="IBM">`, `<product name="SP_QRADAR" vendor="IBM">` oder `<product name="Kaspersky SIEM" vendor="Kaspersky">` den neuen Unterabschnitt `<event>` hinzu und geben Sie anschließend bei Bedarf die weiteren Ereignisattribute ein.

2. Wenn ein Ereignis nur aus gemeinsamen Attributen besteht, bleibt der Unterabschnitt `<event>` leer.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Generation rule for the GNRL_EV_VIRUS_FOUND event with additional
attributes -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
    <product name="Kaspersky SIEM" vendor="Kaspersky">
        <common> <!-- Common Kaspersky Security Center Linux event attributes and corresponding LEEF event
attributes -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

Ereignisse zum Export in SIEM-Systeme im Syslog-Format markieren

Nach der Aktivierung des automatischen Ereignisexports müssen Sie auswählen, welche Ereignisse ins externe SIEM-System exportiert werden sollen.

Sie können den Ereignisexport in das Syslog-Format in ein externes System gemäß einer der folgenden Bedingungen anpassen:

- Allgemeine Ereignisse markieren. Wenn Sie die zu exportierenden Ereignisse in der Richtlinie, in den Einstellungen eines Ereignisses oder in den Einstellungen des Administrationsservers markieren, erhält das SIEM-System die ausgewählten Ereignisse, die in allen Anwendungen auftreten, die von der Richtlinie verwaltet werden. Falls die zu exportierenden Ereignisse in der Richtlinie ausgewählt worden sind, ist es unmöglich, diese für eine einzelne Anwendung, die von dieser Richtlinie verwaltet wird, umzudefinieren.

- Ereignisse für eine verwaltete Anwendung markieren. Wenn Sie die zu exportierenden Ereignisse für eine verwaltete Anwendungen auf einem verwalteten Gerät markieren, werden nur Ereignisse in das SIEM-System übertragen, die in dieser Anwendung aufgetreten sind.

Für die Ereignisse zu Richtlinienänderungen können Sie nur den Export aller dieser Ereignisse in ein SIEM-System aktivieren oder deaktivieren.

Ereignisse von Kaspersky-Anwendungen zum Export im Syslog-Format markieren

Wenn Sie Ereignisse exportieren möchten, die in einer bestimmten verwalteten Anwendung, welche auf den verwalteten Geräten installiert ist, auftreten, markieren Sie in der Anwendungsrichtlinie die Ereignisse für den Export. In diesem Fall werden die markierten Ereignisse von allen Geräten, die sich im Gültigkeitsbereich der Richtlinie befinden, exportiert.

Um zu exportierende Ereignisse für eine bestimmte verwaltete Anwendung zu markieren, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.
2. Klicken Sie auf die Richtlinie der Anwendung, für die Sie die Ereignisse markieren möchten.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.
3. Gehen Sie zum Abschnitt **Konfiguration von Ereignissen**.
4. Aktivieren Sie die Kontrollkästchen neben den Ereignissen, die Sie in ein SIEM-System exportieren möchten.
5. Klicken Sie auf die Schaltfläche **Für den Export in ein SIEM-System mittels Syslog auswählen**.

   Außerdem können Sie im Abschnitt **Ereignisregistrierung**, welcher sich durch Anklicken eines Ereignislinks öffnet, ein Ereignis für den Export in ein SIEM-System markieren.
6. In der Spalte **Syslog** des Ereignisses, oder der Ereignisse, die Sie für den Export in ein SIEM-System markiert haben, erscheint ein Häkchen (✓).
7. Klicken Sie auf die Schaltfläche **Speichern**.

Die markierten Ereignisse aus der verwalteten Anwendung sind für den Export in ein SIEM-System vorbereitet.

Sie können markieren, welche Ereignisse für ein bestimmtes verwaltetes Gerät in ein SIEM-System exportiert werden sollen. Falls bereits früher exportierte Ereignisse in einer Anwendungsrichtlinie markiert wurden, können Sie die markierten Ereignisse für ein verwaltetes Gerät nicht neu definieren.

Um zu exportierende Ereignisse für ein verwaltetes Gerät zu markieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des benötigten Geräts.

   Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.

3. Gehen Sie zum Abschnitt **Anwendungen**.

4. Klicken Sie in der Liste der Anwendungen auf den Link mit dem Namen der benötigten Anwendung.

5. Wechseln Sie zum Abschnitt **Konfiguration von Ereignissen**.

6. Aktivieren Sie die Kontrollkästchen neben den Ereignissen, die Sie nach SIEM exportieren möchten.

7. Klicken Sie auf die Schaltfläche **Für den Export in ein SIEM-System mittels Syslog auswählen**.

   > Außerdem können Sie im Abschnitt **Ereignisregistrierung**, welcher sich durch Anklicken eines Ereignislinks öffnet, ein Ereignis für den Export in ein SIEM-System markieren.

8. In der Spalte **Syslog** des Ereignisses, oder der Ereignisse, die Sie für den Export in ein SIEM-System markiert haben, erscheint ein Häkchen (✓).

Bei konfiguriertem Export in ein SIEM-System sendet der Administrationsserver ab jetzt die ausgewählten Ereignisse an das SIEM-System.

Allgemeine Ereignisse zum Export im Syslog-Format markieren

Sie können allgemeine Ereignisse markieren, die der Administrationsserver unter Verwendung des Syslog-Formats in SIEM-Systeme exportiert.

So markieren Sie Ereignisse für den Export in ein SIEM-System:

1. Führen Sie im Hauptmenü eine der folgenden Aktionen aus:

   - Klicken Sie auf den Namen des Administrationsservers.
   - Wechseln Sie zu **Asset-Verwaltung** → **Richtlinien** und klicken Sie anschließend auf den Link einer Richtlinie.

2. Wechseln Sie im daraufhin geöffneten Fenster auf die Registerkarte **Konfiguration von Ereignissen**.

3. Klicken Sie auf die Schaltfläche **Für den Export in ein SIEM-System mittels Syslog auswählen**.

   > Außerdem können Sie im Abschnitt **Ereignisregistrierung**, welcher sich durch Anklicken eines Ereignislinks öffnet, ein Ereignis für den Export in ein SIEM-System markieren.

4. In der Spalte **Syslog** des Ereignisses, oder der Ereignisse, die Sie für den Export in ein SIEM-System markiert haben, erscheint ein Häkchen (✓).

Bei konfiguriertem Export in ein SIEM-System sendet der Administrationsserver ab jetzt die ausgewählten Ereignisse an das SIEM-System.

Über das Exportieren von Ereignissen im Syslog-Format

Gemäß dem Syslog-Format können Ereignisse, die auf dem Administrationsserver und in den auf den verwalteten Geräten installierten Kaspersky-Anwendungen auftreten, ins SIEM-System exportiert werden.

Syslog ist ein Standardprotokoll zur Registrierung von Nachrichten. Dieses Protokoll ermöglicht, die Software, in der die Nachrichten generiert werden, das System, in dem die Nachrichten gespeichert werden, und die Software, in der die Analysen und die Berichterstellung für die Nachrichten ausgeführt wird, zu trennen. Jeder Nachricht wird der Code des Geräts, der den Typ der Software angibt, mit dessen Hilfe die Nachricht erstellt wurde, und die Signifikanz zugewiesen.

Das Syslog-Format wird in den Dokumenten "Request for Comments" (RFC) definiert, die von der Internet Engineering Task Force veröffentlicht werden. Der Standard RFC 5424 wird für den Ereignisexport aus Kaspersky Security Center Linux in externe Systeme verwendet.

In Kaspersky Security Center Linux können Sie den Ereignisexport in externe Systeme unter Verwendung des Syslog-Formats anpassen.

Der Ablauf des Exports besteht aus zwei Schritten:

1. Aktivierung des automatischen Ereignisexports. In diesem Schritt werden die Einstellungen von Kaspersky Security Center Linux so angepasst, dass der Versand von Ereignissen ins SIEM-System ausgeführt werden kann. Der Versand von Ereignissen aus Kaspersky Security Center Linux beginnt sofort nach der Aktivierung des automatischen Exports.

2. Auswahl der Ereignisse, die ins externe System exportiert werden sollen. In diesem Schritt müssen Sie auswählen, welche Ereignisse ins SIEM-System exportiert werden sollen.

Kaspersky Security Center Linux für den Export von Ereignissen in SIEM-Systeme konfigurieren

Um Ereignisse an ein SIEM-System zu exportieren müssen Sie den Exportprozess in Kaspersky Security Center Linux konfigurieren.

Bevor Ereignisse aus Kaspersky Security Center an ein SIEM-System (QRadar, ArcSight oder Splunk) übertragen werden können, müssen diese Ereignisse in das CEF- oder LEEF-Format konvertiert werden. Dies geschieht unter Verwendung der Regeln, die in der Datei siem_conversion_rules.xml enthalten sind.

So konfigurieren Sie den Export in SIEM-Systeme in Kaspersky Security Center Web Console:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **SIEM-Export** aus.

3. Klicken Sie auf den Link **Einstellungen**.

   Der Abschnitt **Einstellungen exportieren** wird geöffnet.

4. Legen Sie im Abschnitt **Einstellungen exportieren** die Einstellungen fest:

   - **Serveradresse des SIEM-Systems**

     IP-Adresse des Servers, auf dem das verwendete SIEM-System installiert ist. Dieser Wert muss in den Einstellungen des SIEM-Systems genau bestimmt werden.

   - **Port des SIEM-Systems**

     Port, über den eine Verbindung zwischen Kaspersky Security Center Linux und dem Server des SIEM-Systems hergestellt wird. Dieser Wert muss in den Einstellungen von Kaspersky Security Center Linux und in den Einstellungen des Empfängers im SIEM-System angegeben werden.

   - **Protokoll**

     Wählen Sie das Übertragungsprotokoll für Nachrichten ins SIEM-System aus. Sie können das TCP-, UDP- oder TLS-over-TCP-Protokoll auswählen.

     Wenn Sie das Protokoll TLS over TCP auswählen, geben Sie die folgenden TLS-Einstellungen an:

     - **Authentifizierung des Servers**

       In dem Feld **Authentifizierung des Servers** können Sie die **Vertrauenswürdige Zertifikate** oder Werte der **SHA-Fingerabdrücke** auswählen:

       - **Vertrauenswürdige Zertifikate**. Sie können eine vollständige Zertifikatkette (einschließlich des Root-Zertifikats) von einer vertrauenswürdigen Zertifizierungsstelle (Certification Authority – CA) abrufen und diese Datei in Kaspersky Security Center Linux hochladen. Kaspersky Security Center Linux prüft, ob die Zertifikatkette des SIEM-Servers auch von einer vertrauenswürdigen CA signiert ist oder nicht.

         Um ein vertrauenswürdiges Zertifikat hinzuzufügen, klicken Sie auf die Schaltfläche **CA-Zertifikatsdatei auswählen** und laden Sie anschließend das Zertifikat hoch.

       - **SHA-Fingerabdrücke**. Sie können SHA1-Fingerabdrücke der vollständigen Zertifikatkette des SIEM-Systems (einschließlich des Root-Zertifikats) in Kaspersky Security Center Linux angeben. Um einen SHA1-Fingerabdruck hinzuzufügen, geben Sie ihn in das Feld **Fingerabdrücke** ein und klicken Sie anschließend auf die Schaltfläche **Hinzufügen**.

     Durch Verwendung der Einstellung **Client-Authentifizierung hinzufügen** können Sie ein Zertifikat generieren, um Kaspersky Security Center Linux zu authentifizieren. Infolge dessen verwenden Sie ein selbstsigniertes Zertifikat, das von Kaspersky Security Center Linux ausgestellt wurde. In diesem Fall können Sie sowohl ein vertrauenswürdiges Zertifikat als auch einen SHA-Fingerabdruck verwenden, um den SIEM-Systemserver zu authentifizieren.

- **Namen/Alternativen Namen des Antragstellers hinzufügen**

  Der Antragstellername ist ein Domänenname, für den das Zertifikat empfangen wird. Kaspersky Security Center Linux kann keine Verbindung zu dem SIEM-System-Server herstellen, wenn der Domänenname des SIEM-System-Servers nicht mit dem Antragstellernamen des Zertifikats des SIEM-System-Servers übereinstimmt. Der SIEM-Systemserver kann jedoch seinen Domänennamen ändern, wenn sich der Name im Zertifikat geändert hat. In diesem Fall können Sie die Antragstellernamen im Feld **Namen/Alternativen Namen des Antragstellers hinzufügen** angeben. Wenn einer der angegebenen Antragstellernamen mit dem Antragsteller des Zertifikats für das SIEM-Systems übereinstimmt, validiert Kaspersky Security Center Linux das Zertifikat dieses SIEM-Systems.

- **Client-Authentifizierung hinzufügen**

  Um die Client-Authentifizierung durchzuführen, können Sie entweder Ihr Zertifikat einfügen oder es im Kaspersky Security Center Linux generieren.

  - **Zertifikat einfügen**. Sie können ein Zertifikat verwenden, das Sie von einer beliebigen Quelle erhalten haben, beispielsweise von einer vertrauenswürdigen CA. Sie müssen das Zertifikat und seinen privaten Schlüssel angeben, indem Sie einen der folgenden Zertifikat-Typen verwenden:

    - **X.509-Zertifikat im PEM-Format**. Laden Sie jeweils eine Datei mit Zertifikat über das Feld **Datei mit Zertifikat** und eine Datei mit privatem Schlüssel über das Feld **Datei mit Schlüssel** hoch. Beide Dateien sind unabhängig voneinander und die Reihenfolge für das Hochladen der Dateien ist spielt keine Rolle. Wenn beide Dateien hochgeladen sind, geben Sie das Kennwort zum Entschlüsseln des privaten Schlüssels in dem Feld **Überprüfung von Kennwort oder Zertifikat** an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

    - **X.509-Zertifikat im PKCS12-Format**. Laden Sie in dem Feld **Datei mit Zertifikat** eine Datei hoch, die ein Zertifikat und dessen privaten Schlüssel enthält. Geben Sie nach dem Hochladen der Datei das Kennwort zum Entschlüsseln des privaten Schlüssels in dem Feld **Überprüfung von Kennwort oder Zertifikat** an. Das Kennwort kann einen leeren Wert haben, wenn der private Schlüssel nicht verschlüsselt ist.

  - **Schlüssel generieren**. Sie können in Kaspersky Security Center Linux ein selbstsigniertes Zertifikat generieren. Infolge dessen speichert Kaspersky Security Center Linux das generierte selbstsignierte Zertifikat und Sie können den öffentlichen Teil des Zertifikats oder den SHA1-Fingerabdruck an das SIEM-System übergeben.

- **Datumsformat**

  Je nach den Anforderungen des SIEM-Systems können Sie eines der folgenden Formate auswählen: Kaspersky SIEM, IBM QRadar SIEM, ArcSight, Splunk oder Systemprotokolle.

  Wenn Sie das System-Log-Format auswählen, müssen Sie die **Maximale Größe der Nachricht in Byte** angeben.

  Geben Sie die maximale Größe der Nachricht in Byte an, die an das SIEM-System übertragen wird. Jedes Ereignis wird in einer Nachricht übermittelt. Wenn die reale Länge der Nachricht den angegebenen Wert überschreitet, wird die Nachricht abgeschnitten und Daten können verloren gehen. Standardmäßig beträgt die Größe der Nachricht 2048 Bytes. Dieses Feld ist nur verfügbar, falls Sie im Feld **Protokoll** das Format System-Log ausgewählt haben.

5. Wenn Sie möchten, können Sie archivierte Ereignisse aus der Datenbank des Administrationsservers exportieren und das Startdatum angeben, ab dem Sie den Export archivierter Ereignisse starten möchten:

   a. Klicken Sie auf den Link **Geben Sie das Startdatum des Exports an**.

   b. Geben Sie im sich öffnenden Abschnitt das Startdatum im Feld **Exportieren ab dem Startdatum** an.

   c. Klicken Sie auf die Schaltfläche **OK**.

6. Aktivieren Sie die Option **SIEM-Export von Ereignissen**.

7. Bei Bedarf können Sie die Option **SIEM-Export von erweiterten Ereignissen bei Richtlinienänderungen** aktivieren. Für jede geänderte Richtlinieneinstellung wird ein separates Ereignis an SIEM gesendet.

8. Um zu überprüfen, ob die Verbindung mit dem SIEM-System konfiguriert wurde, klicken Sie auf die Schaltfläche **Verbindung prüfen**.

   Die Verbindung mit dem Server des SIEM-Systems wird hergestellt und es wird ein Testereignis gesendet. Der Verbindungsstatus wird angezeigt.

9. Klicken Sie auf die Schaltfläche **Speichern**.

Der Export in ein SIEM-System ist konfiguriert. Wenn Sie in einem SIEM-System das Empfangen von Ereignissen konfiguriert haben, exportiert der Administrationsserver von nun an die markierten Ereignisse oder Ereignisse für Richtlinienänderungen in ein SIEM-System. Wenn Sie das Startdatum des Exports angegeben haben, exportiert der Administrationsserver auch die markierten Ereignisse, die in der Administrationsserver-Datenbank ab dem angegebenen Datum gespeichert sind.

Über das Exportieren von Ereignissen zu Richtlinienänderungen

In Kaspersky Security Center Linux können Sie Ereignisse zu Richtlinienänderungen in ein SIEM-System exportieren. Diese Ereignisse enthalten detaillierte Informationen zu Änderungen an Richtlinien oder Richtlinienprofilen. Diese Informationen können verwendet werden, um den Verlauf von Richtlinienänderungen zu untersuchen und Alarme in SIEM-Systemen zu erstellen.

Auf die Ereignisse zu Richtlinienänderungen kann nur über ein SIEM-System zugegriffen werden.

Die Ereignisse zu Richtlinienänderungen werden nach ihrer Generierung nicht in der Administrationsserver-Datenbank gespeichert und können nicht im Abschnitt **Überwachung → Ereignisauswahlen** der Kaspersky Security Center Web Console angezeigt werden. Außerdem können Sie auf der Registerkarte **Konfiguration von Ereignissen** keine Benachrichtigungseinstellungen und Speichereinstellungen für diese Ereignisse festlegen.

Bedingungen für das Generieren von Ereignissen zu Richtlinienänderungen

In folgenden Fällen werden Ereignisse zu Richtlinienänderungen erstellt:

- Beim Erstellen, Ändern oder Löschen von Richtlinien der folgenden Anwendungen:
  - Kaspersky Security Center Administrationsagent
  - Kaspersky Security Center Administrationsserver
  - Kaspersky Endpoint Security für Windows 14.1

- Wenn die Option **SIEM-Export von erweiterten Ereignissen bei Richtlinienänderungen** in den Eigenschaften des Administrationsservers aktiviert ist.
- Wenn eine Richtlinie manuell über die Benutzeroberfläche der Kaspersky Security Center Web Console geändert wird.

In folgenden Fällen werden keine Ereignisse zu Richtlinienänderungen erstellt:

- Beim Ändern allgemeiner Richtlinieneinstellungen
- Wenn von einer übergeordneten Richtlinie geerbte Richtlinieneinstellungen geändert werden.
- Wenn Richtlinieneinstellungen über die Kaspersky Security Center OpenAPI geändert werden.
- Wenn Einstellungen der Kaspersky-Anwendung direkt in der Anwendung geändert werden.

Parameter für Richtlinienereignisse

Beim Erstellen einer Richtlinie wird für jeden Parameter der Richtlinie ein Ereignis über eine Richtlinienänderung generiert. Beim Ändern einer Richtlinie wird für jeden geänderten Parameter der Richtlinie ein Ereignis über eine Richtlinienänderung generiert. Beim Löschen einer Richtlinie wird ein Ereignis generiert. Beispielsweise werden beim Erstellen einer Richtlinie für Kaspersky Security Center etwa 1.000 Ereignisse und beim Erstellen einer Richtlinie für Kaspersky Endpoint Security mehr als 7.000 Ereignisse generiert.

Die folgende Tabelle enthält eine Reihe von Feldern, die ein Ereignis über eine Richtlinienänderung beschreiben. Die Darstellung dieser Felder ist abhängig vom Ausgabeformat des Ereignisses (z. B. syslog, CEF oder LEEF). Die genauen Feldnamen und Ereignisvorlagen finden Sie in der Datei siem_conversion_rules.xml. Die Ereignisparameter sind nur auf Englisch verfügbar.

Ereignisfeld	Datentyp	Beschreibung
`eventType`	string	Typ des Ereignisses. Ermöglicht das Erstellen von Korrelationsregeln für den bestimmten Typ. Mögliche Werte: "Policy created", "Policy modified", "Policy deleted".
`srvName`	string	Name des Administrationsservers.
`eventTime`	datetime	Datum und Uhrzeit des Ereignisses (Zeitpunkt der Änderung) in UTC.
`eventGroupID`	int	ID der Ereignisgruppe einer Änderung.
`objectID`	int	Interne ID eines Objekts.
`objectName`	string	Anzeigename der Richtlinie.
`objectGroup`	string	Vollständiger Pfad und Name der Administrationsgruppe, in der die Richtlinie enthalten ist.
`user`	string	Name des Benutzers, der die Änderung vorgenommen hat.
`operation`	string	Typ der Parameteränderung. Mögliche Werte: "added", "removed", "changed".
`path`	string	Pfad des Parameters. Enthält den Pfad zum übergeordneten Knoten des Endparameters. Der Pfad wird anhand der Namen der Abschnitte und Unterabschnitte der Richtlinie erstellt. Die Pfadstruktur ist identisch mit den Pfadstrukturen, die in Richtlinieneinstellungen des Administrationsagenten, Allgemeine Richtlinieneinstellungen und Vergleichen von Richtlinienrevisionen beschrieben sind.
`parameter`	string	Name des Endparameters.
`oldValue`	string	Alter Wert des Endparameters.
`newValue`	string	Neuer Wert des Endparameters.

Ereignisse direkt aus der Datenbank exportieren

Sie können die Ereignisse direkt aus der Datenbank von Kaspersky Security Center Linux extrahieren, ohne die Benutzeroberfläche von Kaspersky Security Center Linux zu verwenden. Die Abfragen können unmittelbar in Bezug auf die öffentlichen Ansichten erstellt und von daraus Daten über die Ereignisse extrahiert werden, oder Sie können eigene Ansichten auf der Grundlage der vorhandenen öffentlichen Ansichten erstellen und die gewünschten Daten von dort beziehen.

Öffentlichen Ansichten

Zur Erhöhung der Benutzerfreundlichkeit enthält die Datenbank von Kaspersky Security Center Linux einen Satz mit öffentlichen Ansichten. Eine Beschreibung der öffentlichen Ansichten finden Sie im Dokument klakdb.chm.

Die öffentliche Ansicht v_akpub_ev_event enthält einen Satz Felder, die den Einstellungen der Ereignisse in der Datenbank entsprechen. Im Dokument klakdb.chm finden Sie Informationen über die öffentlichen Ansichten, die sich auf andere Objekte von Kaspersky Security Center Linux beziehen, beispielsweise Geräte, Anwendungen oder Benutzer. Sie können diese Informationen beim Erstellen von Abfragen verwenden.

In diesem Abschnitt finden Sie Anweisungen zum Ausführen einer SQL-Abfrage mithilfe des Tools "klsql2" sowie eine Beispielabfrage.

Sie können auch beliebige andere Datenbankenanwendungen für das Erstellen der SQL-Abfragen und die Datenbankenansichten verwenden. Informationen zum Anzeigen der Einstellungen für die Verbindung mit der Datenbank von Kaspersky Security Center Linux (z. B. Instanz-Name und Name der Datenbank) finden Sie im entsprechenden Abschnitt.

Eine SQL-Abfrage mit dem Tool "klsql2" ausführen

Dieser Artikel enthält die Beschreibung zur Verwendung des Tools "klsql2" sowie zur Ausführung einer SQL-Abfrage mithilfe dieses Tools. Verwenden Sie die Version des Tools "klsql2", die in Ihrem installierten Kaspersky Security Center Linux enthalten ist.

So verwenden Sie das Tool "klsql2":

1. Wechseln Sie in das Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

2. Erstellen Sie in diesem Verzeichnis eine leere Datei mit der sql-Erweiterung.

3. Öffnen Sie die erstellte sql-Datei in einem beliebigen Texteditor.

4. Geben Sie den von Ihnen gewünschten SQL-Query in die sql-Datei ein und speichern Sie die Datei.

5. Geben Sie in der Befehlszeile des Geräts mit dem installierten Administrationsserver den folgenden Befehl zur Ausführung der SQL-Abfrage aus der sql-Datei und die Speicherung der Ergebnisse in der Datei "result.xml" ein:

   ```
   sudo ./klsql2 -i src.sql -u <Benutzername> -p <Kennwort> -o result.xml
   ```

   Wobei `<Benutzername>` und `<Kennwort>` den Anmeldeinformationen des Benutzerkontos entsprechen, das Zugriff auf die Datenbank hat.

6. Geben Sie bei Bedarf den Benutzernamen und das Kennwort des Benutzerkontos ein, das Zugriff auf die Datenbank hat.

7. Öffnen Sie die neu erstellten Dateien des Typs "result.xml" und sehen Sie sich die Ergebnisse der SQL-Abfragen an.

Sie können die sql-Datei editieren und darin beliebige SQL-Anfragen an öffentliche Ansichten erstellen. Die Abfragen können dann mithilfe eines Befehls in der Befehlszeile ausgeführt und die Ergebnisse in einer Datei gespeichert werden.

Beispiel einer SQL-Abfrage, die mit dem Tool "klsql2" erstellt wurde

Dieser Abschnitt enthält eine beispielhafte SQL-Anfrage, die mittels des Tools "klsql2" ausgeführt wurde.

Die folgenden Beispiele zeigen, wie Sie eine Liste mit den Ereignissen auf den Benutzergeräten für die letzten sieben Tage abrufen und diese nach ihrem Eintrittszeitpunkt sortieren. Die aktuellsten Ereignisse werden zuerst angezeigt.

Beispiel für PostgreSQL:

```
SELECT
  /* ID des Ereignisses */
  "e"."nId",

  /* Uhrzeit, zu der das Ereignis aufgetreten ist */
  "e"."tmRiseTime",

  /* interner Name des Ereignistyps */
  "e"."strEventType",

  /* angezeigter Name des Ereignisses */
  "e"."wstrEventTypeDisplayName",

  /* angezeigte Beschreibung des Ereignisses */
  "e"."wstrDescription",

  /* angezeigte Beschreibung des Ereignisses */
  "e"."wstrGroupName",

  /* angezeigter Gerätename des Geräts, auf dem das Ereignis aufgetreten ist */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* IP-Adresse des Gerätes, auf dem das Ereignis aufgetreten ist */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Beispiel für MySQL oder MariaDB

```
SELECT

  /* ID des Ereignisses */
  `e`.`nId`,

  /* Uhrzeit, zu der das Ereignis aufgetreten ist */
  `e`.`tmRiseTime`,

  /* interner Name des Ereignistyps */
  `e`.`strEventType`,

  /* angezeigter Name des Ereignisses */
  `e`.`wstrEventTypeDisplayName`,

  /* angezeigte Beschreibung des Ereignisses */
  `e`.`wstrDescription`,

  /* Name der Gerätegruppe */
  `e`.`wstrGroupName`,

  /* angezeigter Gerätename des Geräts, auf dem das Ereignis aufgetreten ist */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* IP-Adresse des Gerätes, auf dem das Ereignis aufgetreten ist */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Name der Datenbank von Kaspersky Security Center Linux anzeigen

Falls Sie mithilfe von Datenbankverwaltungssystemen für MySQL oder MariaDB auf die Datenbank von Kaspersky Security Center Linux zugreifen möchten, muss der Name der Datenbank bekannt sein, um sie aus dem SQL-Skript-Editor zu verbinden.

Um den Namen der Datenbank von Kaspersky Security Center Linux anzuzeigen:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Details der aktuellen Datenbank** aus.

Der Datenbankname wird im Feld **Name der Datenbank** angegeben. Verwenden Sie diesen Namen der Datenbank für die Verbindung und den Zugriff auf die Datenbank in Ihren SQL-Abfragen.

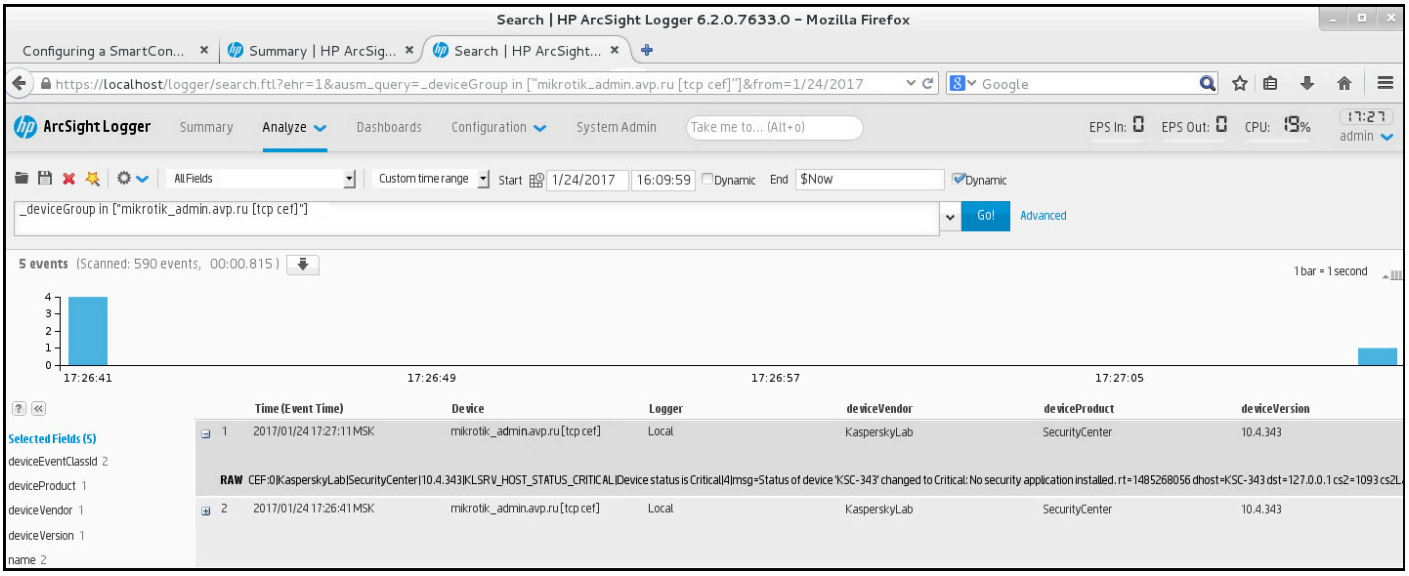
Exportergebnisse anzeigen

Sie können erfahren, ob die Exportprozedur erfolgreich fertig gestellt wurde. Überprüfen Sie dazu, ob das SIEM-System die Nachrichten, in denen die exportierten Ereignisse enthalten sind, erhalten hat.

Wenn die aus Kaspersky Security Center Linux versendeten Ereignisse erhalten und vom SIEM-System richtig interpretiert wurden, bedeutet das, dass die Konfiguration auf beiden Seiten korrekt ausgeführt wurde. Andernfalls prüfen Sie und korrigieren Sie erforderlichenfalls die Einstellungen in Kaspersky Security Center Linux und im SIEM-System.

Nachfolgend finden Sie ein Beispiel für Ereignisse, die ins ArcSight-System exportiert wurden. Das erste Ereignis ist beispielsweise ein kritisches Ereignis des Administrationsservers: "*Gerätestatus ist Kritisch*".

Die Anzeige der exportierten Ereignisse ist vom verwendeten SIEM-System abhängig.



Beispiel für Ereignisse

Umgang mit Objekt-Revisionen

Der Abschnitt enthält Informationen über die Arbeit mit den Revisionen des Objekts. Kaspersky Security Center Linux erlaubt eine Nachverfolgung der Änderungen von Objekten. Jedes Mal, wenn Sie die Änderungen des Objektes speichern, wird eine *Revision* erstellt. Jede Revision hat eine Nummer.

Folgende Objekte unterstützen die Arbeit mit Revisionen:

- Eigenschaften des Administrationsservers
- Richtlinien
- Aufgaben
- Administrationsgruppen
- Benutzerkonten
- Installationspakete

Sie können mit den Revisionen von Objekten folgende Aktionen ausführen:

- Eine ausgewählten Revision anzeigen (nur für Richtlinien)
- Ein Rollback der Objektänderungen auf eine ausgewählte Revision durchführen
- Revisionen in einer JSON-Datei speichern (nur für Richtlinien)

Im Eigenschaftenfenster der Objekte, die den Umgang mit Revisionen unterstützen, wird im Abschnitt **Revisionsverlauf** eine Liste der Objektrevisionen mit den folgenden Informationen angezeigt:

- **Revision** – Nummer der Revision des Objekts
- **Uhrzeit** – Datum und Uhrzeit der Objektänderung
- **Benutzer** – Name des Benutzers, der das Objekt geändert hat
- **IP-Adresse des Benutzergeräts** – IP-Adresse des Geräts, von dem aus das Objekt geändert wurde.
- **IP-Adresse der Web Console** – IP-Adresse der Kaspersky Security Center Web Console, mit der das Objekt geändert wurde.
- **Aktion** – Aktion, die auf das Objekt angewendet wurde
- **Beschreibung** – Informationen zu den Änderungen der Objekteinstellungen für diese Revision

  Standardmäßig ist die Beschreibung der Revision des Objekts nicht ausgefüllt. Um eine Beschreibung der Revision hinzuzufügen, wählen Sie die gewünschte Revision aus und klicken Sie auf die Schaltfläche **Beschreibung bearbeiten**. Geben Sie im neuen Fenster einen Text zur Beschreibung der Revision ein.

Revision einer Richtlinie anzeigen und speichern

In Kaspersky Security Center Linux können Sie anzeigen, welche Änderungen an einer Richtlinie in einem bestimmten Zeitraum vorgenommen wurden, und Informationen über diese Änderungen in einer Datei speichern.

Anzeige und Speichern einer Richtlinienrevision sind verfügbar, wenn diese Funktionalität durch das entsprechende Verwaltungs-Web-Plug-in unterstützt wird.

So zeigen Sie eine Richtlinienrevision an:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.
2. Klicken Sie auf die Richtlinie, deren Revision Sie anzeigen möchten, und gehen Sie dann zum Abschnitt **Revisionsverlauf**.
3. Klicken Sie in der Liste mit den Richtlinienrevisionen auf die Nummer der Revision, die Sie anzeigen möchten.

   Wenn die Revision größer als 10 MB ist, können Sie diese in der Kaspersky Security Center Web Console nicht anzeigen. Sie werden aufgefordert, die ausgewählte Revision in einer JSON-Datei zu speichern.

Wenn die Revision nicht größer als 10 MB ist, werden die Einstellungen der ausgewählten Richtlinienrevision als Bericht im HTML-Format angezeigt. Der Bericht wird in einem Pop-up-Fenster angezeigt. Daher müssen Sie sicherstellen, dass das Anzeigen von Pop-ups in Ihrem Browser erlaubt ist.

Für die Richtlinien von Kaspersky Endpoint Security für Windows und Kaspersky Endpoint Security for Mac enthält der Bericht keine Informationen über die Richtlinienprofile.

So speichern Sie eine Richtlinienrevision als JSON-Datei:

Wählen Sie in der Liste der Richtlinienrevisionen die Revision aus, die Sie speichern möchten, und klicken Sie dann auf **In Datei speichern**.

Die Revision wird in einer JSON-Datei gespeichert.

Bei Bedarf können Sie Richtlinienrevisionen vergleichen. Diese Option ist für die Richtlinien der folgenden Komponenten verfügbar: Administrationsserver, Administrationsagent, Kaspersky Endpoint Security für Windows (beginnend ab Version 14.0 des Web-Plug-ins) und Kaspersky Endpoint Security for Mac (beginnend ab Version 12.2.1 Patch A des Web-Plug-ins).

Richtlinienrevisionen vergleichen

Sie haben die folgenden Vergleichsmöglichkeiten: Vergleich von früheren Revisionen einer Richtlinie mit der aktuellen Version, Vergleich verschiedener in der Liste ausgewählter Revisionen untereinander und Vergleich einer Revision einer Richtlinie mit einer Revision einer anderen Richtlinie. Die Optionen sind für Richtlinien der folgenden Komponenten verfügbar: Administrationsserver, Administrationsagent, Kaspersky Endpoint Security für Windows (beginnend ab Version 14.0 des Web-Plug-ins) und Kaspersky Endpoint Security for Mac (beginnend ab Version 12.2.1 Patch A des Web-Plug-ins).

So zeigen Sie eine Richtlinienrevision an:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.
2. Klicken Sie auf die Richtlinie, deren Revisionen Sie vergleichen möchten.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.
3. Wechseln Sie zur Registerkarte **Revisionsverlauf** und aktivieren Sie die Kontrollkästchen neben den zu vergleichenden Versionen.

4. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Vergleichen** und wählen Sie anschließend eine der folgenden Optionen aus der Dropdown-Liste:

   - **Mit aktueller Revision**, wenn Sie die in Schritt 3 ausgewählte Revision mit der zuletzt gespeicherten Revision der gleichen Richtlinie vergleichen möchten.

   - **Ausgewählte Revisionen**, wenn Sie die zwei Revisionen vergleichen möchten, deren Kontrollkästchen Sie in Schritt 3 aktiviert haben.

     Die Reihenfolge, in der die Kontrollkästchen aktiviert werden, hat keinen Einfluss auf das Vergleichsergebnis. Standardmäßig wird die frühere Revision der ausgewählten Revision mit der neuesten Revision verglichen. Wenn Sie beispielsweise die Kontrollkästchen neben den Revisionen 5 und 1 auswählen, wird Revision 1 mit Revision 5 verglichen. Der Bericht enthält Informationen über jene Einstellungen in Revision 1, die im Vergleich zu Revision 5 hinzugefügt, entfernt oder geändert wurden.

   - **Mit anderer Richtlinienrevision**, wenn Sie die Revisionen von zwei verschiedenen Richtlinien vergleichen möchten.

     Führen Sie im neu geöffneten rechten Bereich Folgendes aus:

     a. Wählen Sie im Feld **Anwendungsname** die Richtlinie aus, die Sie vergleichen möchten: Administrationsagent oder Administrationsserver.

     b. Geben Sie im Feld **Richtlinienname** den Namen der Richtlinie an, deren Revision Sie mit der in Schritt 3 ausgewählten Revision vergleichen möchten.

        Die Liste der Richtlinienrevisionen wird angezeigt.

     c. Wählen Sie die erforderliche Revision aus und klicken Sie auf die Schaltfläche **Vergleichen**.

In einem neuen Tab Ihres Browsers wird ein Bericht über den Revisionsvergleich im HTML-Format angezeigt.

Wenn das Ergebnis des Vergleichs 10 MB überschreitet, wird ein entsprechender Dialog angezeigt. Sie können entweder auf die Schaltfläche **Als Datei speichern** klicken, um den Bericht als Datei zu speichern, oder den Vorgang abbrechen.

Der Bericht wird in der Sprache angezeigt, die in der Benutzeroberfläche Ihrer Kaspersky Security Center Web Console verwendet wird. Sie können einzelne Abschnitte des Berichts erweitern, indem Sie auf das Symbol mit dem Pfeil nach unten (▾) neben dem Abschnitt klicken. Durch Anklicken des Symbols mit dem Pfeil nach oben (▴) können Sie erweiterte Abschnitte wieder ausblenden.

Der Bericht enthält die folgenden Informationen:

- Kaspersky-Logo.
- Den Namen des Berichts.
- Die Uhrzeit und das Datum der Berichtserstellung.
- Den Richtliniennamen, den Administrationsserver und die Administrationsgruppe, welche die Richtlinie bzw. die Richtlinien, deren Revisionen verglichen werden, enthalten.
- Die Schaltfläche **Als HTML speichern**. Wenn Sie diese Schaltfläche anklicken, wird der Bericht auf Ihrem Computer gespeichert.

- Den Abschnitt **Zusammenfassung**, der die allgemeinen Informationen zu den verglichenen Revisionen anzeigt: Name der Richtlinie bzw. der Richtlinien, Nummer der Revision, Uhrzeit und Datum der gespeicherten Revision, Benutzer der gespeicherten Revision und Beschreibung zur Revision.

  Für geerbte Richtlinien wird kein Benutzer angezeigt.

- Unterschiede zwischen den verglichenen Revisionen. Die Unterschiede werden in den folgenden Abschnitten dargestellt:

  - **Hinzugefügte Einstellungen**
  - **Entfernte Einstellungen**
  - **Geänderte Einstellungen**
  - **Einstellungen, die nur für Objekt 1 verfügbar sind** (Wenn Sie die Revisionen zweier verschiedener Richtlinien verglichen haben)
  - **Einstellungen, die nur für Objekt 2 verfügbar** sind (Wenn Sie die Revisionen zweier verschiedener Richtlinien verglichen haben)

  Wenn ein Abschnitt keine Daten enthält, wird er nicht angezeigt.

Für die Richtlinien von Kaspersky Endpoint Security für Windows und Kaspersky Endpoint Security for Mac enthält der Bericht über den Revisionsvergleich keine Informationen über die Richtlinienprofile.

Objekte auf eine frühere Version zurück rollen

Falls erforderlich können Sie an einem Objekt vorgenommene Änderungen zurücksetzen. Beispielsweise kann es erforderlich sein, die Einstellungen der Richtlinie auf den Zustand eines bestimmten Datums zurückzusetzen.

So setzen Sie e an einem Objekt vorgenommene Änderungen zurück:

1. Wählen Sie im Eigenschaftenfenster des Objekts die Registerkarte **Revisionsverlauf** aus.
2. Wählen Sie in der Liste mit den Revisionen des Objekts die Revision aus, auf deren Stand die Änderungen zurückgesetzt werden sollen.
3. Klicken Sie auf die Schaltfläche **Rollback**.
4. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

   Das Objekt wird auf die ausgewählte Revision zurückgesetzt. In der Liste der Revisionen des Objektes wird ein Eintrag über die ausgeführte Aktion angezeigt. In der Beschreibung der Revision werden die Informationen über die Nummer der Revision angezeigt, auf die Sie das Objekt zurückgesetzt haben.

Das Zurücksetzen von Revisionen ist nur für Richtlinien- und Aufgabenobjekte verfügbar.

Aktive Bedrohungen

Informationen über unverarbeitete Dateien, die sich auf den Client-Geräten befinden, finden Sie im Abschnitt **Datenverwaltung** im Unterabschnitt **Aktive Bedrohungen**.

Die verschobene Verarbeitung und die Desinfektion von Dateien mithilfe der Sicherheitsanwendung werden auf Befehl oder nach Eintreten eines bestimmten Ereignisses ausgeführt. Sie können Einstellungen der verschobenen Desinfektion von Dateien anpassen.

Unverarbeitete Dateien desinfizieren

Um die Desinfektion einer unverarbeiteten Datei zu starten, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Datenverwaltung** → **Aktive Bedrohungen**.
2. führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen neben der Datei, die Sie desinfizieren müssen.
   - Klicken Sie auf den Namen der Datei, die Sie desinfizieren müssen.
3. Starten Sie die Desinfektion der Datei, indem Sie auf die Schaltfläche **Desinfizieren** klicken.

   Anschließend wird versucht, die ausgewählte Datei zu desinfizieren.

Wenn die Datei desinfiziert wurde, stellt die auf dem Client-Gerät installierte Sicherheitsanwendung die Datei im ursprünglichen Ordner wieder her. Der Eintrag für diese Datei wird aus der Liste im Abschnitt **Aktive Bedrohungen** gelöscht. Wenn eine Desinfektion der Datei nicht möglich ist, löscht die auf dem Gerät installierte Sicherheitsanwendung die Datei vom Gerät. Der Eintrag für diese Datei wird aus der Liste im Abschnitt **Aktive Bedrohungen** gelöscht.

Die Möglichkeiten zur Desinfektion und Löschung von Dateien können je nach installierter Sicherheitsanwendung, Version und Einstellungen variieren.

Unverarbeitete Dateien herunterladen

Kaspersky Security Center Linux ermöglicht Ihnen das Herunterladen von Kopien unverarbeiteter Dateien, die auf den Client-Geräten gefunden wurden. Dies bezieht sich auf Dateien, die von der Anwendung desinfiziert oder gelöscht wurden. Die Dateien werden auf das Gerät mit Kaspersky Security Center Linux in den von Ihnen angegebenen Ordner heruntergeladen.

Sie können Kopien von Dateien herunterladen, wenn Dateien im Zuge ihrer Desinfektion gelöscht oder verändert wurden. Die Kopien dieser Dateien werden auf dem verwalteten Gerät im Speicher von Kaspersky Endpoint Security für Linux abgelegt.

So laden Sie die Kopie einer unverarbeiteten Datei herunter:

1. Wechseln Sie im Hauptmenü zu **Datenverwaltung** → **Aktive Bedrohungen**.
2. Führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen neben der Datei, die Sie herunterladen müssen.
   - Klicken Sie auf den Namen der Datei, die Sie herunterladen müssen.
3. Um den Download zu starten, klicken Sie auf die Schaltfläche **Herunterladen**.

Daraufhin lädt die Sicherheitsanwendung des Client-Geräts, auf dem die ausgewählte unverarbeitete Datei gefunden wurde, eine Kopie der Datei in den angegebenen Ordner herunter.

Dateien aus dem Abschnitt "Aktive Bedrohungen" löschen

*So löschen Sie Dateien aus dem Abschnitt **Aktive Bedrohungen**:*

1. Wechseln Sie im Hauptmenü zu **Datenverwaltung** → **Aktive Bedrohungen**.
2. führen Sie eine der folgenden Aktionen aus:
   - Aktivieren Sie das Kontrollkästchen neben der Datei, die Sie löschen müssen.
   - Klicken Sie auf den Namen der Datei, die Sie löschen müssen.
3. Löschen Sie die Dateien, indem Sie auf die Schaltfläche **Löschen** klicken.
4. Klicken Sie in dem folgenden Fenster auf die Schaltfläche **Löschen**.

   Daraufhin werden diese Dateien, die von den Sicherheitsanwendungen in die Datenverwaltung der Client-Geräte verschoben wurden, aus der jeweiligen Datenverwaltung gelöscht. Die Einträge für diese Dateien werden aus der Liste im Abschnitt **Aktive Bedrohungen** gelöscht.

Löschen von Objekten

Dieser Abschnitt enthält Informationen über das Löschen von Objekten.

Sie können Objekte löschen, einschließlich der folgenden:

- Richtlinien
- Aufgaben
- Installationspakete
- Virtuelle Administrationsserver
- Benutzer

- Sicherheitsgruppen
- Administrationsgruppen

Um ein Objekt zu löschen, gehen Sie wie folgt vor:

1. Öffnen Sie den erforderlichen Bereich in der Kaspersky Security Center Web Console und wählen Sie anschließend das Objekt aus.
2. Klicken Sie in der Werkzeugleiste auf die Schaltfläche **Löschen**.
3. Klicken Sie im folgenden Fenster auf **OK**, um die Auswahl zu bestätigen.

   Das ausgewählte Objekt wird gelöscht.

Wenn Sie ein Objekt löschen, verbleiben die Informationen darüber in der Datenbank. Die Speicherdauer für Informationen über die gelöschten Objekte ist identisch mit der Speicherdauer für Revisionen des Objekts (die empfohlenen Dauer beträgt 90 Tage). Sie können die Speicherdauer nur ändern, wenn Sie über die Berechtigung **Ändern** im Berechtigungsbereich **Gelöschte Objekte** verfügen.

Über das Löschen von Client-Geräten

Wenn Sie ein verwaltetes Gerät aus einer Administrationsgruppe löschen, verschiebt die Anwendung das Gerät in die Gruppe "Nicht zugeordnete Geräte". Nach dem Löschen des Geräts verbleiben der installierte Administrationsagent und die Kaspersky-Sicherheitsanwendungen, wie Kaspersky Endpoint Security, auf dem Gerät.

Kaspersky Security Center Linux geht mit den Geräten in der Gruppe "Nicht zugeordnete Geräte" gemäß den folgenden Regeln um:

- Wenn Sie Verschiebungsregeln für Geräte konfiguriert haben und ein Gerät die Kriterien einer Verschiebungsregel erfüllt, wird das Gerät automatisch gemäß dieser Regel in eine Administrationsgruppe verschoben.
- Das Gerät wird in der Gruppe "Nicht zugeordnete Geräte" gespeichert und gemäß den Aufbewahrungsregeln für Geräte automatisch aus der Gruppe entfernt.

  Die Aufbewahrungsregeln für Geräte wirken sich nicht auf Geräte aus, in denen Laufwerke mit vollständiger Festplattenverschlüsselung verschlüsselt sind. Solche Geräte werden nicht automatisch gelöscht, sondern können nur manuell gelöscht werden. Wenn Sie ein Gerät mit einem verschlüsselten Laufwerk löschen müssen, entschlüsseln Sie zuerst das Laufwerk und löschen Sie anschließend das Gerät.

  Wenn Sie ein Gerät mit einem verschlüsselten Laufwerk löschen, werden auch die zum Entschlüsseln des Laufwerks erforderlichen Daten gelöscht. Wenn Sie im Bestätigungsfenster, das sich öffnet, wenn Sie solche Geräte löschen (entweder aus der Gruppe **Nicht zugeordnete Geräte** oder aus der Gruppe **Verwaltete Geräte**), das Kontrollkästchen **Ich kenne das Risiko und möchte die ausgewählten Geräte löschen** aktivieren, geben Sie an, dass Sie von der anschließenden Datenlöschung Kenntnis haben.

Um das Laufwerk zu entschlüsseln, müssen die folgenden Bedingungen erfüllt sein:

- Das Gerät wird erneut mit dem Administrationsserver verbunden, um die zum Entschlüsseln des Laufwerks erforderlichen Daten wiederherzustellen.
- Der Benutzer des Geräts merkt sich das Kennwort zum Entschlüsseln.
- Die Sicherheitsanwendung, mit der das Laufwerk verschlüsselt wurde (z. B. Kaspersky Endpoint Security für Windows), ist weiterhin auf dem Gerät installiert.

Wenn das Laufwerk mittels Kaspersky-Festplattenverschlüsselung verschlüsselt wurde, können Sie auch versuchen, die Daten mithilfe des Wiederherstellungs-Tools FDERT wiederherzustellen.

Wenn Sie ein Gerät mit verschlüsselten Laufwerken in einer VDI-Umgebung besitzen, werden die Informationen auf dem verschlüsselten Laufwerk gelöscht, nachdem Sie das Gerät gelöscht haben.

Wenn Sie ein Gerät manuell aus der Gruppe "Nicht zugeordnete Geräte" löschen, entfernt die Anwendung das Gerät aus der Liste. Nach dem Löschen des Geräts verbleiben etwaige installierte Kaspersky -Anwendungen auf dem Gerät. Wenn das Gerät für den Administrationsserver weiterhin sichtbar ist und Sie die regelmäßige Netzwerkabfrage konfiguriert haben, erkennt Kaspersky Security Center Linux das Gerät während der Netzwerkabfrage und fügt es erneut der Gruppe "Nicht zugeordnete Geräte" hinzu. Daher ist es sinnvoll, ein Gerät nur dann manuell zu löschen, wenn es für den Administrationsserver unsichtbar ist.

Dateien aus Quarantäne und Datei-Backups herunterladen und löschen

Dieser Abschnitt enthält Informationen zum Herunterladen und Löschen von Dateien aus Quarantäne und Datei-Backups in der Kaspersky Security Center Web Console.

Dateien aus der Quarantäne und von Datei-Backups herunterladen

Sie können Dateien aus der Quarantäne und den Datei-Backups nur herunterladen, wenn eine der beiden Bedingungen erfüllt ist: Entweder ist die Option **Verbindung mit Administrationsserver nicht trennen** in den Geräteeinstellungen aktiviert, oder es wird ein Verbindungsgateway verwendet. Andernfalls ist der Download nicht möglich.

So speichern Sie die Kopie einer Datei aus der Quarantäne oder dem Datei-Backups auf einer Festplatte:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie eine Kopie der Datei aus der Quarantäne speichern wollen, wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Quarantäne**.

   - Wenn Sie eine Kopie der Datei aus dem Backup speichern möchten, wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Datei-Backups**.

2. Wählen Sie in dem sich öffnenden Fenster eine Datei aus, die Sie herunterladen möchten und klicken Sie auf **Herunterladen**.

Der Download wird gestartet. Eine Kopie der Datei, die sich in der Quarantäne des Client-Geräts befindet, wird im angegebenen Order gespeichert.

Über das Entfernen von Objekten aus den Datenverwaltungen der Quarantäne, des Datei-Backups oder der aktiven Bedrohungen

Wenn die auf den Client-Geräten installierten Sicherheitsanwendungen von Kaspersky Objekte in die Datenverwaltungen von Quarantäne, Backup oder der aktiven Bedrohungen platzieren, senden sie Informationen darüber an die Abschnitte **Quarantäne**, **Datei-Backups**, oder **Aktive Bedrohungen** von Kaspersky Security Center Linux. Wenn Sie einen dieser Abschnitte öffnen, können Sie das gewünschte Objekt entfernen.

Wählen Sie für die Abschnitte **Datei-Backups** oder **Aktive Bedrohungen** ein Objekt aus der Liste und klicken Sie auf die Schaltfläche **Entfernen**.

Für den Abschnitt **Quarantäne** können Sie eine der folgenden Aktionen ausführen:

- Aktivieren Sie das Kontrollkästchen neben dem Namen des zu entfernenden Objekts und klicken Sie anschließend in der Symbolleiste auf die Schaltfläche **Löschen**.

- Klicken Sie auf den Namen des zu entfernenden Objekts und klicken Sie im angezeigten Detailfenster in der Symbolleiste auf die Schaltfläche **Löschen**.

  In diesem Fall wird das Objekt gelöscht, eine entsprechende Benachrichtigung auf dem Bildschirm angezeigt und das Detailfenster geschlossen.

Kaspersky Security Center Linux entfernt entweder das ausgewählte Objekt aus der Liste oder löscht das ausgewählte Objekt aus der Datenverwaltung. Die auszuführende Aktion wird durch die Kaspersky-Anwendung festgelegt, die das ausgewählte Objekt in der Datenverwaltung abgelegt hat. Die Kaspersky-Anwendung ist im Feld **Eintrag hinzugefügt von** angegeben.

Weitere Informationen darüber, welche Aktion ausgeführt werden soll, finden Sie in der Dokumentation der Kaspersky-Anwendung.

Die Anwendung über SNMP verwalten

In diesem Abschnitt wird beschrieben, wie Sie mithilfe von SNMP (Simple Network Management Protocol) unter Linux Informationen vom Administrationsserver abrufen.

SNMP ist ein Protokoll zur Verwaltung von Netzwerkgeräten.

Für die SNMP-Kommunikation verwendet Kaspersky Security Center Linux den im Betriebssystem vorhandenen snmp-Dienst und einen SNMP-Agenten, um die Leistung des Administrationsservers zu überwachen und Daten mithilfe von OIDs an Anwendungen zu senden. Kaspersky Security Center Linux kann diese Informationen in Form von Statistiken oder SNMP-Traps (Benachrichtigungen über Anwendungsereignisse) senden.

Mittels SNMP können Sie auf folgende Anwendungsinformationen zugreifen:

- Allgemeine Informationen
- Statistiken von Kaspersky Security Center Linux ab dem Zeitpunkt der Anwendungsinstallation
- Informationen über Ereignisse von Kaspersky Security Center Linux

Es wird nur Lesezugriff gewährt.

Informationen zu SNMP-Traps und Statistiken, die über SNMP gesendet werden, werden in der Datei "adminkit.mib" gespeichert. Standardmäßig befindet sich die Datei "adminkit.mib" im Ordner /opt/kaspersky/ksc64/share/snmp/.

Der lokale snmpd-Dienst auf jedem Cluster-Knoten dient als SNMP-Server, der die Statistiken empfängt. Die Interaktion mit einem externen SNMP-Server wird nicht unterstützt. SNMP-Traps können lokal auf jedem Cluster-Knoten mithilfe des Dienstes snmptrapd empfangen oder an einen externen Server umgeleitet werden.

Um Vorgänge über SNMP auszuführen, müssen Sie den snmpd-Dienst im Betriebssystem auf jedem Cluster-Knoten vorkonfigurieren.

Den SNMP-Dienst im Betriebssystem konfigurieren

Stellen Sie vor der Konfiguration sicher, dass der snmpd-Dienst in Ihrem Betriebssystem installiert ist.

Erstellen eines Benutzerkontos für den Zugriff auf die Daten

Bevor Sie das Konto erstellen, stoppen Sie den snmpd-Dienst mit folgendem Befehl:
bash
sudo systemctl stop snmpd

Um die Sicherheit des Datenzugriffs über SNMPv3 mit Authentifizierung und Verschlüsselung zu gewährleisten, müssen Sie auf der Seite des snmpd-Dienstes ein Benutzerkonto mit folgenden Informationen erstellen:

- Benutzername (Groß-/Kleinschreibung berücksichtigen)
- Authentifizierungsalgorithmus (MD5 oder SHA, SHA wird empfohlen)
- Authentifizierungskennwort
- Verschlüsselungsalgorithmus (unterstützt nur AES)
- Verschlüsselungskennwort

Sie können ein Benutzerkonto durch folgende Methoden erstellen:

- Durch Verwendung des Tools "net-snmp-create-v3-user", sofern dieses im Betriebssystem verfügbar ist.
- Manuell durch Hinzufügen der entsprechenden Direktive zur Konfigurationsdatei des snmpd-Dienstes.

Um ein Benutzerkonto mittels des Tools "net-snmp-create-v3-user" zu erstellen, führen Sie folgenden Befehl aus:

```
net-snmp-create-v3-user -ro -a <Authentifizierungsalgorithmus> -x <Verschlüsselungsalgorithmus> <Benutzername>
```

Die Authentifizierungs- und Verschlüsselungskennwörter werden interaktiv abgefragt.

Beispiele:

```
net-snmp-create-v3-user -ro -a SHA -x AES MonitoringUser
```

So erstellen Sie eine Benutzerrolle manuell:

1. Erstellen Sie die Konfigurationsdatei "/var/lib/snmp/snmpd.conf", indem Sie folgenden Befehl ausführen:

   ```
   touch /var/lib/snmp/snmpd.conf
   ```

2. Fügen Sie der Datei die folgenden Zeilen hinzu:

   ```
   createUser <Benutzername> <Authentifizierungsalgorithmus> "<Authentifizierungskennwort>"
   <Verschlüsselungsalgorithmus> "<Verschlüsselungskennwort>"
   ```

   Beispiele:

   ```
   createUser MonitoringUser SHA "MonitoringAuthSecret" AES "MonitoringPrivSecret"
   ```

Erstellen eines Benutzerkontos zum Empfangen von SNMP-Traps

Um SNMP-Traps über SNMPv3 mit Authentifizierung und Verschlüsselung zu empfangen, müssen Sie ein Konto auf der Seite des Überwachungssystems im Kontext des entsprechenden Dienstes (in der Regel des snmptrapd-Dienstes) erstellen.

Das Konto muss die folgenden Informationen enthalten:

- Benutzername
- Authentifizierungsalgorithmus
- Authentifizierungskennwort
- Verschlüsselungsalgorithmus
- Verschlüsselungskennwort

> Aus Sicherheitsgründen sollten separate Benutzerkonten für den Datenzugriff und den Empfang von SNMP-Traps verwendet werden.

Anweisungen zum Erstellen eines Benutzerkontos zum Empfangen von SNMP-Traps finden Sie in der Dokumentation Ihres Überwachungssystems.

Konfiguration des snmpd-Dienstes

Die Konfiguration des snmpd-Dienstes ist in der Datei "/etc/snmp/snmpd.conf" gespeichert. Sie können die erforderlichen Informationen in eine bestehende Konfigurationsdatei einfügen oder eine neue Konfigurationsdatei erstellen und die unten aufgeführten Zeilen in der angegebenen Reihenfolge hinzufügen.

> Wenn Sie eine neue Konfigurationsdatei erstellen, stellen Sie sicher, dass nur der Superuser Zugriff darauf hat.

So konfigurieren Sie den SNMP-Dienst:

1. Geben Sie in der Konfigurationsdatei das Protokoll, die Adresse der Netzwerkschnittstelle und die Portnummer an, auf welcher der snmpd-Dienst auf eingehende Anfragen warten soll.

   - Um Anfragen auf allen Netzwerkschnittstellen zu empfangen, fügen Sie der Konfigurationsdatei die folgenden Zeilen hinzu:

     ```
     agentAddress udp:161
     ```

   - Um lediglich Anfragen auf der lokalen Netzwerkschnittstelle zu empfangen, z. B. wenn das Überwachungssystem auf demselben Rechner installiert ist, fügen Sie der Konfigurationsdatei die folgenden Zeilen hinzu:

     ```
     agentAddress udp:127.0.0.1:161
     ```

2. Konfigurieren Sie die Interaktion zwischen dem Kaspersky Security Center Linux und dem SNMP-Dienst. Sie können entweder einen UNIX-Socket oder einen TCP-Socket verwenden.

   - Bei Verwendung eines UNIX-Sockets:

     a. Geben Sie Pfad und Berechtigungen für den UNIX-Socket an: Fügen Sie dafür der Konfigurationsdatei die folgenden Zeilen hinzu:

     ```
     master agentx
     agentXSocket unix:/var/run/agentx-master.socket
     agentXPerms 770 770 kluser klusers
     ```

     b. Fügen Sie die Gruppe "klusers" als zusätzliche Gruppe für das Konto {'KLSRV_UNATT_KLSVCUSER'} hinzu.

   - Geben Sie bei Verwendung eines TCP-Sockets den Port und die Adresse für den TCP-Socket an. Fügen Sie dafür der Konfigurationsdatei die folgenden Zeilen hinzu:

     ```
     master agentx
     agentXSocket tcp:127.0.0.1:705,tcp6:[::1]:705
     ```

3. Legen Sie für das minimale Antwort-Timeout mindestens 30 Sekunden fest. Fügen Sie dafür der Konfigurationsdatei die folgenden Zeilen hinzu:

   ```
   agentxTimeout 30
   ```

4. Bei Bedarf, können Sie eine Beschreibung des Servers mit konfiguriertem SNMP, den Standort des Systems und die Kontaktadresse des Administrators angeben. Fügen Sie dafür der Konfigurationsdatei die folgenden Zeilen hinzu:

   ```
   sysDescr <Serverbeschreibung>
   sysLocation <Serverstandort>
   sysContact <Kontaktadresse des Administrators>
   sysServices 72
   ```

5. Geben Sie den Bereich des OID-Trees an, der Ihrem Überwachungssystem über das SNMP-Protokoll zur Verfügung stehen soll. Fügen Sie dafür der Konfigurationsdatei die folgenden Zeilen hinzu:

   ```
   view monitoring included .1.3.6.1.4.1.23668.1093.1

   view systemonly included .1.3.6.1.4.1.23668.1093.1
   ```

6. Bei Bedarf können Sie den Bereich des OID-Trees, der die vom snmpd-Dienst gespeicherten Informationen über das Betriebssystem enthält, zusätzlich festlegen. Dieser Bereich steht Ihrem Überwachungssystem zur Verfügung.

Zu den Informationen über das Betriebssystem gehören beispielsweise Angaben zu folgenden Metriken: CPU- und RAM-Auslastung, freier Speicherplatz auf Festplattenpartitionen, Auslastung der Netzwerkschnittstellen, Liste installierter Software, Liste offener Netzwerkverbindungen und Liste laufender Prozesse. Ein Teil dieser Informationen kann vertraulich sein.

- Wenn Sie lediglich den Zugriff auf allgemeine Systeminformationen und Angaben zur Nutzung von RAM, CPU und Festplatten erlauben möchten, fügen Sie der Konfigurationsdatei die folgenden Zeilen hinzu:

```
# SNMPv2-MIB - Basic system information
view monitoring included .1.3.6.1.2.1.1
# HOST-RESOURCES-MIB - CPU, Memory, Filesystems
view monitoring included .1.3.6.1.2.1.25.1
view monitoring included .1.3.6.1.2.1.25.2
view monitoring included .1.3.6.1.2.1.25.3
view monitoring included .1.3.6.1.2.1.25.5
# UCD-SNMP-MIB - Memory and CPU usage
view monitoring included .1.3.6.1.4.1.2021.4
view monitoring included .1.3.6.1.4.1.2021.10
view monitoring included .1.3.6.1.4.1.2021.11
# UCD-SNMP-DISKIO-MIB - Block devices I/O statistics
view monitoring included .1.3.6.1.4.1.2021.13
# IF-MIB - Network interfaces I/O statistics
view monitoring included .1.3.6.1.2.1.2
view monitoring included .1.3.6.1.2.1.31
```

- Um Zugriff auf alle Systeminformationen zu gewähren, fügen Sie der Konfigurationsdatei die folgenden Zeilen hinzu:

```
view monitoring included .1
```

7. Legen Sie den Zugriffsmodus und den Umfang an Informationen für das erstellte Benutzerkonto fest. Fügen Sie dafür der Konfigurationsdatei die folgenden Zeilen hinzu:

```
rouser <user name> priv -V monitoring
```

8. Um SNMP-Traps zu senden, geben Sie die IP-Adresse des Überwachungssystems und die Anmeldeinformationen des Benutzers zum Empfangen der Traps an. Fügen Sie dafür der Konfigurationsdatei die folgenden Zeilen hinzu:

```
trapsess -Ci -v3 -t0.1 -r1 -l authPriv -u <Benutzername zum Empfangen von Traps> -a
<Authentifizierungsalgorithmus> -A "<Benutzerkennwort zum Empfangen von Traps>" -x
<Verschlüsselungsalgorithmus> -X "<Verschlüsselungskennwort>" udp:<IP-Adresse>:162
```

Der snmpd-Dienst ist konfiguriert.

Um mehrere Überwachungssysteme zu integrieren, erstellen Sie für jedes System ein separates Benutzerkonto, legen Sie den Umfang der verfügbaren Informationen für jedes Benutzerkonto fest (via "view"- und "rouser"-Direktive) und konfigurieren Sie das Senden von SNMP-Traps (via "trapsess"-Direktive).

Starten des snmpd-Dienstes mit der neuen Konfiguration

Um die neue Konfiguration anzuwenden:

1. Starten Sie den snmpd-Dienst neu:

   ```
   systemctl restart snmpd
   ```

2. Überprüfen Sie den Status des snmpd-Dienstes:

   ```
   systemctl status snmpd
   ```

   Der Status muss `running` lauten.

3. Erlauben Sie den Autostart des Dienstes beim Hochfahren des System:

   ```
   systemctl enable snmpd
   ```

4. Wenn Sie in Ihrem Betriebssystem oder Netzwerkgerät eine Firewall verwenden, fügen Sie Regeln hinzu, um die SNMP-Pakete durchzulassen.

Der snmp-Dienst wird ausgeführt.

Wenn der klcssnmp-Dienst während der Konfiguration des snmpd-Dienstes ausgeführt wurde, starten Sie den klcssnmp-Dienst ebenfalls neu.

Überprüfen des Zustands des snmp-Dienstes

Um den snmpd-Dienst zu testen, konfigurieren Sie in Kaspersky Security Center Linux die Verwendung von SNMP und fordern Sie mit dem Tool "snmpwalk" SNMP-Daten an.

Um den Umfang der von Kaspersky Security Center Linux bereitgestellten SNMP-Daten zu erhalten,

führen Sie den folgenden Befehl aus:

```
snmpwalk -v3 -l authPriv -u <Benutzername> -a <Authentifizierungsalgorithmus> -A "<Authentifizierungskennwort>" -x
<Verschlüsselungsalgorithmus> -X "<Verschlüsselungskennwort>" <IP-Adresse> .1.3.6.1.4.1.23668.1093.1
```

Beispiele:

```
snmpwalk -v3 -l authPriv -u MonitoringUser -a SHA -A "MonitoringAuthSecret" -x AES -X "MonitoringPrivSecret"
127.0.0.1 .1.3.6.1.4.1.23668.1093.1
```

Benachrichtigung per SNMP aktivieren und deaktivieren

Kaspersky Security Center Linux sendet Benachrichtigungen über Ereignisse des Administrationsservers in Form von SNMP-Traps.

Standardmäßig sind SNMP-Benachrichtigungen für die Ereignisse von Kaspersky Security Center Linux deaktiviert.

Um Benachrichtigungen per SNMP für Ereignisse von Kaspersky Security Center Linux zu aktivieren oder deaktivieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das **Eigenschaften des Administrationsservers** wird geöffnet.

2. Klicken Sie in der Registerkarte **Konfiguration von Ereignissen** des Eigenschaftenfensters auf den Ereignistyp, für den Sie SNMP-Benachrichtigungen erhalten möchten.

3. Im neuen Bereich können Sie den Schalter **Per SNMP benachrichtigen** aktivieren oder deaktivieren.

   Diese Option ist nur verfügbar, wenn die Option **Statistiken über SNMP senden** aktiviert ist.

Die SNMP-Benachrichtigungen für Ereignisse von Kaspersky Security Center Linux werden entsprechend Ihrer Auswahl aktiviert oder deaktiviert.

SNMP in Kaspersky Security Center Linux aktivieren und deaktivieren

Standardmäßig ist das Senden von Statistiken über SNMP aktiviert. Um SNMP-Traps zu senden, konfigurieren Sie den snmpd-Dienst.

Um das Senden von Statistiken über SNMP zu aktivieren oder zu deaktivieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das **Eigenschaften des Administrationsservers** wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **über SNMP**.

3. Aktivieren oder deaktivieren Sie den Umschalter **Statistiken über SNMP senden**.

4. Klicken Sie auf **Speichern**.

Das Senden von Statistiken über SNMP ist entsprechend Ihrer Auswahl aktiviert oder deaktiviert.

Werte von Objektkennungen für SNMP

In der folgenden Tabelle sind die Werte und Beschreibungen der Objektkennungen (auch als OIDs bezeichnet) aufgeführt, die zum Übertragen von Informationen über die Leistung des Administrationsservers an Drittanbieter-Anwendungen verwendet werden.

Werte und Beschreibungen von Objektkennungen für SNMP

Wert der Objektkennung	Numerischer Datentyp	OID	Beschreibung
`deploymentStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.1.1	Bereitstellungsstatus. Es gibt folgende Statusvarianten: • **Information**. Die Lizenz gilt nicht mehr für n Geräte. • **Warnung**. Eine der folgenden Varianten: Es gibt Geräte mit installierten Kaspersky-Anwendungen auf insgesamt n Geräten in den Administrationsserver-Gruppen (n > m). Lizenz L läuft auf n Geräten in m Tagen ab. Aufgabe T für die Installation von Anwendungen wurde auf n Geräten erfolgreich abgeschlossen. Für m Geräte ist ein Neustart erforderlich. • **Kritisch**. Die Lizenz ist für n Geräte abgelaufen. • **OK**. Keine der oben genannten Varianten.
`noAntivirusSoftware`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.1	`deploymentStatus` gibt an, dass die Administrationsserver-Gruppe zu viele Geräte ohne verwaltete Anwendungen enthält. Der Wert ist 1, wenn einige Geräte ohne verwaltete Anwendungen gefunden wurden. Andernfalls ist der Wert 0.
`remoteInstallTaskFailed`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.2	`deploymentStatus` gibt an, dass die Aufgabe zur Remote-Installation auf einigen Geräten fehlgeschlagen ist. Die Anzahl dieser Geräte kann mit `hostsRemoteInstallFailed` abgerufen werden.
`licenceExpiring`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.3	`deploymentStatus` gibt an, dass Geräte existieren, auf denen die Lizenz innerhalb den nächsten 7 Tagen abläuft. Die Anzahl dieser Geräte kann mit `hostsLicenseExpiring` abgerufen werden.
`licenceExpired`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.1.2.4	`deploymentStatus` gibt an, dass es Geräte mit einer abgelaufenen Lizenz gibt. Die Anzahl dieser Geräte können Sie mit `hostsLicenseExpired` abrufen.
`hostsInGroups`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.3	Anzahl der Geräte in den Administrationsserver-Gruppen
`hostsWithAntivirus`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.4	Anzahl der Geräte mit installierten verwalteten Programmen in den Administrationsserver-Gruppen.
`hostsRemoteInstallFailed`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.5	Anzahl der Geräte, auf denen die Aufgabe zur Remote-Installation fehlgeschlagen ist.
`licenceExpiringSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.6	ID eines Lizenzschlüssels, der in weniger als 7 Tagen abläuft.
`licenceExpiredSerial`	`OCTET STRING`	.1.3.6.1.4.1.23668.1093.1.1.7	ID des abgelaufenen Lizenzschlüssels.
`licenceExpiringDays`	`Unsigned32`	.1.3.6.1.4.1.23668.1093.1.1.8	Anzahl der Tage bis zum Ablauf der Lizenz. Für diesen Parameter gilt der Lizenzzeitraum als abgelaufen, wenn bis zum Ablaufdatum weniger als 7 Tage verbleiben. Wenn bis zum Ablaufdatum mehr als 7 Tage verbleiben, ist der Wert des Parameters "0".
`hostsLicenceExpiring`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.9	Anzahl der Geräte mit einer Lizenz, die in weniger als 7 Tagen abläuft.
`hostsLicenceExpired`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.1.10	Anzahl der Geräte mit einer abgelaufenen Lizenz.

Wert der Objektkennung	Numerischer Datentyp	OID	Beschreibung
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	Aktueller Status des Updates der Antiviren-Datenbanken. Es gibt folgende Statusvarianten: • **Information**. Die Antiviren-Datenbanken auf dem Administrationsserver oder auf den Geräten wurden seit mehr als 1 Tag nicht aktualisiert und Programm wurde vor weniger als 1 Tag installiert. • **Warnung**. Die Antiviren-Datenbanken auf dem Administrationsserver oder auf den Geräten wurden seit mehr als 3 Tagen nicht aktualisiert. Dieser Wert kann in den Gruppeneinstellungen geändert werden. • **Kritisch**. Die Antiviren-Datenbanken auf dem Administrationsserver oder auf den Geräten wurden seit mehr als 7 Tagen nicht aktualisiert. Dieser Wert kann in den Gruppeneinstellungen geändert werden. • **OK**. Keine der oben genannten Varianten.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	Das letzte Update des Administrationsservers liegt lange zurück. Die als "lang" angesehene Zeit wird in `updatesStatus` festgelegt.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Einige Geräte wurden über längere Zeit nicht aktualisiert (standardmäßig nach 3 Tagen **Warnung** und nach 7 Tagen **Kritisch**). Die Anzahl dieser Geräte können Sie mit `hostsNotUpdated` abrufen.
lastServerUpdateTime	Hex-STRING	.1.3.6.1.4.1.23668.1093.1.2.3	Letzter Zeitpunkt der Aktualisierung der Antiviren-Datenbanken auf dem Administrationsserver.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Anzahl der Geräte, deren Antiviren-Datenbanken für längere Zeit nicht aktualisiert wurden (standardmäßig nach 3 Tagen **Warnung** und nach 7 Tagen **Kritisch**). Sollten Geräte den Update-Status **Kritisch** besitzen, werden nur diese Geräte gezählt. Den Update-Status können Sie mittels `updatesStatus` abrufen.
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	Status des Echtzeitschutzes. Eine der folgenden Varianten: • **Warnung**. Eine der folgenden Varianten: Auf einem Gerät, das zur Administrationsserver-Gruppe gehört, wird eine Sicherheitsverletzung festgestellt. Aufgrund von Verschlüsselungsfehlern wurde für einige Geräte der Schutzstatus geändert. Die letzte vollständige Untersuchung liegt lange zurück. • **Kritisch**. Der Antiviren-Schutz funktioniert auf einigen Geräten in den Administrationsserver-Gruppen nicht. • **OK**. Keine der oben genannten Varianten.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Auf einigen Geräten wird keine Sicherheitsanwendung ausgeführt. Die Anzahl dieser Geräte können Sie mit `hostsAntivirusNotRunning` abrufen.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	Auf einigen Geräten wird der Echtzeitschutz nicht ausgeführt. Die Anzahl dieser Geräte können Sie mit `hostsRealtimeNotRunning` abrufen.
psRealtimeLevelChanged	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.3	Während der Laufzeit weicht die Schutzstufe von der vom Administrator auf n Computern in Administrationsgruppen festgelegten Stufe ab.
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Es gibt Geräte, die nicht desinfizierte Objekte enthalten. Die Anzahl dieser Geräte können Sie mit `hostsNotCuredObject` abrufen.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Auf einigen Geräten wurden Bedrohungen gefunden. Die Anzahl dieser Geräte können Sie mit `hostsTooManyThreats` abrufen.

Wert der Objektkennung	Numerischer Datentyp	OID	Beschreibung
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	Der Status des Virenangriffs auf dem System. Der Wert ist gleich 1, wenn während einer bestimmten Zeit eine bestimmte Anzahl von Viren gefunden wurde, andernfalls 0. Die Anzahl der Viren und die Zeitdauer werden auf dem Administrationsserver mithilfe der Einstellungen für `Virenangriffe` angegeben.
psVulnerabilitiesFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.7	Es wurden Schwachstellen gefunden.
psEncryptionFaultsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.8	Es wurden Fehler bei der Verschlüsselung erkannt, die den Schutzstatus des Geräts geändert haben.
psVulnerableHostsFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.9	Auf einigen Geräten wurden Schwachstellen gefunden.
psNotScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.10	Es wurden Geräte gefunden, für die längere Zeit keine vollständige Untersuchung durchgeführt wurde.
psNagentsNotRunningUntilReboot	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.11	Es wurden Geräte gefunden, auf denen der Administrationsagent erst nach einem Neustart ausgeführt wird.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Anzahl der Geräte, auf denen keine Sicherheitsanwendungen ausgeführt werden.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Anzahl der Geräte, auf denen der Echtzeitschutz die nicht ausgeführt wird.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Anzahl der Geräte mit einer inakzeptablen Stufe des Echtzeitschutzes.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Anzahl der Geräte, die nicht desinfizierte Objekte enthalten.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Anzahl der Geräte, die Bedrohungen enthalten.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	Der Status der vollständigen Untersuchung auf Viren ist einer der folgenden: • **Information**. Seit der Installation des Programms sind weniger als 7 Tage vergangen. • **Warnung**. Nach der Programminstallation wurde länger als 7 Tage keine vollständige Untersuchung auf Viren durchgeführt. • **Kritisch**. Nach der Programminstallation wurde länger als 14 Tage keine vollständige Untersuchung auf Viren durchgeführt. • **OK**. Keine der oben genannten Varianten.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Einige Geräte wurden seit einer gewissen Zeit nicht untersucht. Die Anzahl dieser Geräte können Sie mit `hostsNotScannedLately` abrufen. Die Zeitdauer wird in `fullScanStatus` angegeben.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Anzahl der Geräte, die in einem bestimmten Zeitraum nicht untersucht wurden. Die Zeitdauer wird in `fullScanStatus` angegeben.
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	Status des logischen Netzwerks des Administrationsservers. Eine der folgenden Varianten: • **Warnung**. Wenn Geräte, auf die kein Zugriff besteht, einen Status des Typs "Warnung" besitzen, oder wenn Geräte existieren, die keiner Administrationsserver-Gruppe angehören. • **Kritisch**. Wenn es Geräte gibt, deren Kontrolle der Administrationsserver verloren hat, oder wenn es Geräte mit einem kritischen Status gibt und auf die nicht zugegriffen werden kann. • **OK**. Keine der oben genannten Varianten.

Wert der Objektkennung	Numerischer Datentyp	OID	Beschreibung
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Einige Geräte waren längere Zeit nicht mit dem Administrationsserver verbunden (7 Tage oder länger für ein Gerät mit dem Status **Warnung** und 4 Tage für ein Gerät mit dem Status **Kritisch**). Die Anzahl dieser Geräte können Sie mit hostsNotConnectedLongTime abrufen.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	Es gibt Geräte, die nicht mehr vom Administrationsserver kontrolliert werden. Die Anzahl dieser Geräte können Sie mit hostsControlLost abrufen.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Anzahl der vom Administrationsserver gefundenen Geräte, die keiner Administrationsserver-Gruppe angehören.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Anzahl der Gruppen des Administrationsservers.
hostsNotConnectedLongTime	Counter32	.1.3.6.1.4.1.23668.1093.1.5.5	Anzahl der Geräte, die längere Zeit nicht mit dem Administrationsserver verbunden waren. Die als "lang" angesehene Zeit wird in notConnectedLongTime festgelegt.
hostsControlLost	Counter32	.1.3.6.1.4.1.23668.1093.1.5.6	Anzahl der Geräte, die nicht vom Administrationsserver kontrolliert werden.
eventsStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.6.1	Status des Ereignis-Subsystems ist einer der folgenden: • **Warnung**. Eine der folgenden Varianten: Geräte Administrationsserver-Gruppe haben lange nicht mehr nach Windows-Updates gesucht. Es gibt Geräte mit Statusproblemen. • **Kritisch**. Eine der folgenden Varianten: Auf mindestens einem Gerät liegt ein Ereignis mit der Priorität "Kritisch" vor. Auf mindestens einem Gerät liegt ein Ereignis mit der Priorität "Error" vor. Es gibt ein Ereignis, das besagt, dass eine Aufgabe auf mindestens einem Gerät nicht erfolgreich abgeschlossen wurde. Geräte Administrationsserver-Gruppe haben lange nicht mehr nach Windows-Updates gesucht. Es gibt Geräte mit Statusproblemen. • **Information.** Eine der folgenden Varianten: Alle Geräte wurden vor weniger als einer Woche vollständig auf Viren untersucht. Die Remote-Installationsaufgaben sind abgeschlossen und kein Gerät muss neu gestartet werden. Das letzte Update des Administrationsservers liegt weniger als eine Woche zurück. Der Administrationsserver erhielt lange keine Updates, wird aber gerade aktualisiert. • **OK**. Keine der oben genannten Varianten.
criticalEventOccured	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.6.2.1	eventsStatus zeigt, dass auf dem Administrationsserver einige kritische Ereignisse vorliegen. Die Anzahl dieser Ereignisse können Sie mit criticalEventsCount abrufen. Der Wert ist gleich 1, wenn auf einem beliebigen Gerät mindestens ein kritisches Ereignis vorliegt, andernfalls ist der Wert 0.
criticalEventsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.6.3	Anzahl der kritischen Ereignisse auf dem Administrationsserver.

Arbeiten mit Kaspersky Security Center Linux unter der Lizenz für Kaspersky Next XDR Optimum

Wenn Sie eine Lizenz für Kaspersky Next XDR Optimum als Teil einer EPP-Anwendungslizenz und einer Lizenz für Kaspersky Security Center Linux erworben haben, können Sie die Funktionalität von Kaspersky Next XDR Optimum nach der Erstkonfiguration nutzen.

Wenn Sie nach der Installation und Aktivierung von Kaspersky-Anwendungen auf Geräten eine Lizenz für Kaspersky Next XDR Optimum separat als Erweiterung einer zuvor erworbenen Lizenz erworben haben, müssen Sie je nachdem, wie Sie die Lizenz für Kaspersky Next XDR Optimum erworben haben, Kaspersky Security Center Linux auf den Geräten mithilfe des neuen Aktivierungscodes oder der Schlüsseldatei reaktivieren. Anschließend können Sie die Erstkonfiguration durchführen.

Darüber hinaus können Sie die Funktionen von Kaspersky Next XDR Optimum im Testmodus nutzen. Dafür müssen Sie zunächst einen sekundären physischen Administrationsserver hinzufügen und diesen Server anschließend unter Ihrer Testlizenz für Kaspersky Next XDR Optimum aktivieren. Die Funktionen von Kaspersky Next XDR Optimum stehen während der Gültigkeitsdauer Ihrer Demolizenz auf dem sekundären Server zur Verfügung.

Nachdem Sie den Administrationsserver unter Ihrer Lizenz von Kaspersky Next XDR Optimum aktiviert und den Lizenzschlüssel an die verwalteten Geräte des entsprechenden Administrationsservers verteilt haben, können Sie Folgendes tun:

- Reagieren Sie auf Bedrohungen, indem Sie Integrationen mit Kaspersky Automated Security Awareness Platform, Kaspersky Threat Intelligence Portal Sandbox und Active Directory vornehmen.
- Alarme nach Attributen gruppieren.

Weitere Informationen zu den Funktionen, die durch die Lizenz für Kaspersky Next XDR Optimum aktiviert werden, finden Sie in der Hilfe zu Kaspersky Endpoint Detection and Response Optimum.

Integrationen für die Reaktion auf Alarme

Wenn Sie über die Lizenz für Kaspersky Next XDR Optimum verfügen, können Sie Integrationen mit den folgenden Lösungen konfigurieren, um auf Bedrohungen zu reagieren:

- Kaspersky Automated Security Awareness Platform
- Kaspersky Threat Intelligence Portal Sandbox
- Active Directory

Diese Integrationen sind verfügbar, wenn Sie den Administrationsserver unter einer Lizenz für Kaspersky Next XDR Optimum aktiviert haben.
Um Reaktionsmaßnahmen auszuführen, müssen Sie den Lizenzschlüssel für Kaspersky Next XDR Optimum für Ihre verwalteten Anwendungen bereitstellen.
Wenn Sie die Funktionen von Kaspersky Next XDR Optimum unter einer Demolizenz verwenden, müssen Sie zunächst einen sekundären physischen Administrationsserver hinzufügen, diesen sekundären Administrationsserver unter der Demolizenz aktivieren und anschließend den Lizenzschlüssel auf die Geräte verteilen, die von diesem Administrationsserver verwaltet werden.

Wenn Sie die Lizenz für Kaspersky Next EDR Optimum verwenden, müssen Sie die Anwendungen, die auf Ihren verwalteten Geräten installiert sind, nicht unter der Lizenz für Kaspersky Next XDR Optimum aktivieren. Sie müssen dies nur für neue Geräte tun (falls vorhanden).

Da die Lizenz von Kaspersky Next XDR Optimum Mandantenfähigkeit unterstützt, können Sie den Lizenzschlüssel zentral an verwaltete Anwendungen verteilen. Die automatische Verteilung der Lizenz auf sekundäre und virtuelle Administrationsserver wird nicht unterstützt.

Um die Integrationen zu konfigurieren, müssen Sie über die Berechtigungen **Lesen** und **Schreiben** für den Funktionsbereich **Allgemeine Funktionen: Anwendungsintegration** verfügen.

Integration mit Active Directory für die Ausführung von Reaktionsmaßnahmen konfigurieren

Die Integration mit Active Directory ermöglicht es Ihnen, Reaktionsmaßnahmen für Active Directory-Benutzer auszuführen, die vom Alarm betroffen oder daran beteiligt sind.

Um die Integration mit Active Directory für die Reaktion auf Alarme zu konfigurieren, müssen Sie den Kaspersky Security Center Linux Administrationsserver Version 15.4 oder höher verwenden.

Die Integration mit Active Directory für die Reaktion auf Alarme und die Einstellungen für die Untersuchung des Active Directory-Domänencontrollers (Adresse und Anmeldeinformationen des Domänencontrollers), die Sie bei der Konfiguration der Abfrage des Domänencontrollers angeben, sind zwei verschiedene Einstellungen. Da Sie sicherstellen müssen, dass der Benutzer, für den eine Reaktionsmaßnahme ausgeführt werden soll, über ein Active Directory-Konto verfügt, müssen Sie beide Integrationen konfigurieren: für die Untersuchung und für die Reaktion. Die Reihenfolge spielt dabei keine Rolle.

Die Integrationseinstellungen werden nicht vererbt und nur auf den Administrationsserver (physisch oder virtuell) angewendet, auf dem Sie diese Einstellungen konfigurieren.

Gehen Sie wie folgt vor, um die Integration mit Active Directory für die Reaktion auf Alarme zu konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Führen Sie eine der folgenden Aktionen aus:

   - Wählen Sie den Abschnitt **Verteilungspunkte** aus, klicken Sie auf den Namen des gewünschten Verteilungspunkts und wählen Sie anschließend im folgenden Eigenschaftenfenster den Abschnitt **Active Directory** aus.

   - Wählen Sie den Bereich **Active Directory-Antwort** aus.

3. Aktivieren Sie im rechten Bereich den Umschalter **Integration von Active Directory**.

   Wenn Sie die Integration später deaktivieren möchten, können Sie dies nur für alle Verbindungen tun, indem Sie den Umschalter **Integration von Active Directory** deaktivieren. Sie können die Integration nicht für eine einzelne Verbindung deaktivieren. Stattdessen können Sie die Verbindung löschen.

   > Wenn Sie den Umschalter **Integration von Active Directory** aktivieren oder deaktivieren, wird die Einstellung sowohl für den Abschnitt **Active Directory-Antwort** als auch für den Abschnitt **Verteilungspunkte** übernommen.

4. Stellen Sie eine Verbindung zum Active Directory-Domänencontroller her, indem Sie auf die Schaltfläche **Hinzufügen** klicken.

5. Passen Sie im nächsten Fenster die folgenden Parameter für die Verbindung an:

   - **Adresse des Domänencontrollers**

     Name des Computers, z. B. `server.mycompany.com`.

     Sie können mehrere Adressen angeben. Alle Domänencontroller, deren Adressen Sie angeben, müssen zu derselben Domäne gehören.

   - **Name der Active Directory-Domäne**

     Vollständig qualifizierter DNS-Domänenname, z. B. `mycompany.com`

     Sie können auch den SAM- oder NetBIOS-Namen angeben, z. B. `mycompany`

     Verwenden Sie Kleinbuchstaben. Wenn Sie mehrere Verbindungen für den Administrationsserver oder einen Verteilungspunkt erstellen, geben Sie für jede Verbindung einen anderen Namen an.

     > Um Reaktionsmaßnahmen durchzuführen, muss der in diesem Feld angegebene Active Directory-Domänenname mit dem im Alarm angegebenen Active Directory-Domänennamen übereinstimmen.

   - **Anmelden**

     Benutzername des Active Directory-Kontos mit Administratorrechten, unter dem die Reaktionsmaßnahmen ausgeführt werden sollen.

   - **Kennwort**

     Kennwort des Active Directory-Kontos mit Administratorrechten, unter dem die Reaktionsmaßnahmen ausgeführt werden sollen.

6. Wenn Sie den Verbindungsstatus überprüfen möchten, klicken Sie auf die Schaltfläche **Verbindung prüfen**.

   Wenn die Verbindung erfolgreich hergestellt wurde, wird der Status **Verbunden** angezeigt. Andernfalls lautet der Status **Fehlgeschlagen** und es wird eine Fehlermeldung für die Domänencontroller angezeigt, zu denen Sie keine Verbindung herstellen konnten.

> Sie müssen berücksichtigen, wie Sie eine Verbindung mit Active Directory herstellen: **von einem Linux-Gerät oder von einem Windows-Gerät**.

Verbindung von einem Linux-Gerät herstellen

Wenn Sie sich von einem Linux-Gerät aus mit einem Domänencontroller verbinden und sich bei ihm authentifizieren, sieht die Logik standardmäßig wie folgt aus:

1. Der Administrationsserver oder ein Verteilungspunkt versucht, über LDAPS eine Verbindung mit dem Domänencontroller herzustellen.

   Es wird eine strenge Überprüfung des LDAP-Serverzertifikats durchgeführt.

2. Um das Zertifikat zu validieren, legen Sie den öffentlichen Teil des Domänencontroller-Zertifikats im Zertifikatsspeicher des Systems ab.

   Für den Zugriff auf die Zertifikatskette wird der vom Betriebssystem abhängige Pfad zur Zertifizierungsstelle (CA) des Systems verwendet.

   Beispielsweise:

   - /etc/ssl/certs/ca-certificates.crt – Pfad für Debian-basierte Betriebssysteme (Debian, Ubuntu, Astra).
   - /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem – Pfad für CentOS oder Red Hat.

3. Wenn die LDAP-Verbindung fehlschlägt, tritt ein Fehler auf und es wird kein anderes Verbindungsprotokoll verwendet.

> Bei Problemen mit LDAP können Sie sich an den Technischen Support von Kaspersky wenden.

Wenn Sie das Zertifikat nicht im Zertifikatsspeicher des Systems installieren möchten, können Sie das Flag KLNAG_LDAP_SSL_CACERT verwenden, um den Pfad zum Domänencontroller-Zertifikat festzulegen. Führen Sie dazu folgenden Befehl aus:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "</path/to/domain-controller/cert>"
```

wobei `</path/to/domain-controller/cert>` der Pfad zum öffentlichen Teil des Domänencontroller-Zertifikats ist.

Wenn der Pfad beispielsweise `"/var/opt/kaspersky/ldap_cert.crt"` lautet, lautet der Befehl `klscflag -fset -pv klnagent -n KLNAG_LDAP_SSL_CACERT -t s -v "/var/opt/kaspersky/ldap_cert.crt"`

Verbindung von einem Windows-Gerät herstellen

Wenn Sie sich von einem Windows-Gerät aus mit einem Domänencontroller verbinden und sich bei diesem authentifizieren, werden die Verbindungseinstellungen von der Domäne festgelegt.

Sie müssen nur Folgendes sicherstellen:

- LDAPS ist aktiviert und Port 636 ist auf dem Gerät verfügbar.
- Sie erlauben Verbindungen zum Domänencontroller durch eine Firewall oder einen Proxyserver.

7. Klicken Sie auf **Speichern**.

Das Fenster wird geschlossen und die Verbindung wird in der Verbindungstabelle angezeigt.

In der Verbindungstabelle sind folgende Aktionen möglich:

- Verbindungsparameter bearbeiten.

  Klicken Sie dazu für die gewünschte Verbindung auf den Link mit dem Parameter **Adresse des Domänencontrollers**. Ändern Sie im neuen Fenster die gewünschten Einstellungen und klicken Sie anschließend auf die Schaltfläche **Speichern**.

  Sie können nur die Parameter **Anmelden** und **Kennwort** bearbeiten.

- Verbindungen löschen.

  Aktivieren Sie dazu das Kontrollkästchen neben der Verbindung, die Sie löschen möchten, klicken Sie auf die Schaltfläche **Entfernen** in der Werkzeugleiste und bestätigen Sie anschließend das Löschen der Verbindung.

Integration mit der Kaspersky Automated Security Awareness Platform konfigurieren

Die Integration in die Kaspersky Automated Security Awareness Platform (im Folgenden auch KASAP genannt) ermöglicht die Zuordnung von KASAP-Lernkursen für Benutzer, die mit Alarmen verknüpft sind.

Die Integrationseinstellungen werden nicht vererbt und nur auf den Administrationsserver (physisch oder virtuell) angewendet, auf dem Sie diese Einstellungen konfigurieren.

Bevor Sie eine Integration in Kaspersky Security Center Web Console konfigurieren können, müssen Sie einen Autorisierungs-Token erstellen und eine URL für API-Anfragen in KASAP anfordern.

Gehen Sie wie folgt vor, um die Integration mit der Kaspersky Automated Security Awareness Platform zu konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wählen Sie den Abschnitt **KASAP** aus.

3. Aktivieren Sie im rechten Bereich den Umschalter **KASAP-Integration**.

4. Geben Sie die Einstellungen an, die für die Verbindung mit KASAP verwendet werden sollen:

   - **API-Token**: Token, das Sie für den Zugriff auf die Open API von KASAP erstellt haben.
   - **URL**: URL für API-Anfragen, die Sie beim Erstellen des API-Tokens erhalten haben.

- **Proxyserver verwenden**: Umschalter, der die Verwendung eines Proxyservers für die Verbindung mit KASAP aktiviert.

  Der Umschalter ist standardmäßig deaktiviert.

5. Überprüfen Sie gegebenenfalls Ihre Einstellungen, indem Sie auf die Schaltfläche **Verbindung prüfen** klicken.

   Der Verbindungsstatus wird angezeigt.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Die Integration mit der Kaspersky Automated Security Awareness Platform ist konfiguriert.

Nachdem die Einstellungen der KASAP-Integration gespeichert wurden, können Sie die Liste der KASAP-Lerngruppen anzeigen, indem Sie auf die Schaltfläche **Gruppen anzeigen** klicken.

Wenn die Gruppenliste angezeigt wird, können Sie sie bei Bedarf aktualisieren, indem Sie auf die Schaltfläche **Gruppen aktualisieren** klicken.

Die Liste kann nach dem Öffnen nicht ausgeblendet werden. Wenn Sie den Umschalter für die **KASAP-Integration** deaktivieren, wird die Liste der KASAP-Gruppen nicht angezeigt.

Integration mit Kaspersky Threat Intelligence Portal Sandbox konfigurieren

Die Integration mit Kaspersky Threat Intelligence Portal (im Folgenden auch Kaspersky TIP genannt) ermöglicht die Ausführung der Dateien, die mithilfe von Kaspersky Sandbox in die **Quarantäne** verschoben wurden – eine sichere Umgebung, die von Ihrem Unternehmensnetzwerk isoliert ist.

Die Integrationseinstellungen werden nicht vererbt und nur auf den Administrationsserver (physisch oder virtuell) angewendet, auf dem Sie diese Einstellungen konfigurieren.

Bevor Sie die Integration konfigurieren, müssen Sie ein Autorisierungs-Token für API-Anfragen auf Kaspersky TIP anfordern.

Gehen Sie wie folgt vor, um die Integration mit Kaspersky TIP Sandbox zu konfigurieren:

1. Klicken Sie im Hauptmenü auf den Namen des Administrationsservers.

   Das Fenster mit den Einstellungen des Administrationsservers wird geöffnet, in welchem die Registerkarte **Allgemein** ausgewählt ist.

2. Wählen Sie **Kaspersky TIP** aus.

3. Aktivieren Sie im rechten Bereich den Umschalter **Integration**.

   Die Einstellungen für die Verbindung mit Kaspersky TIP werden angezeigt.

   Wenn Sie nach dem Konfigurieren und Speichern der Integrationseinstellungen den Umschalter **Integration** deaktivieren, werden die Einstellungen nicht gelöscht, aber Sie können die Reaktionsmaßnahme nicht ausführen.

4. Klicken Sie auf die Schaltfläche **Token hinzufügen**, geben Sie im angezeigten Fenster das Token an, das Sie zuvor über Kaspersky TIP erhalten haben, und klicken Sie dann auf die Schaltfläche **Hinzufügen**.

   Das Fenster wird geschlossen und das API-Token wird hinzugefügt.

5. Wenn Sie für die Verbindung mit Kaspersky TIP einen Proxyserver verwenden möchten, aktivieren Sie den Umschalter **Proxyserver verwenden**.

   Der Umschalter ist standardmäßig deaktiviert.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Die Integration mit Kaspersky TIP Sandbox ist konfiguriert.

Jetzt können Sie Dateien aus der **Quarantäne** zur Bedrohungsanalyse an Kaspersky TIP Sandbox senden. Die maximale Größe einer Datei beträgt 100 MB.

Da die Lizenz für Kaspersky Next XDR Optimum die Mandantenfähigkeit unterstützt, können Dateien, die in die **Quarantäne** verschoben werden, nach Mandanten aufgeteilt werden. Diese Trennung auf Mandantenebene kann auch für das Senden von Dateien an Kaspersky TIP Sandbox und die Anzeige der Ergebnisse angewendet werden, wenn der Administrator ein dediziertes TIP-Konto und ein API-Token für jeden Mandanten verwendet. Eine zentrale Verwaltung des Abschnitts **Quarantäne** für alle Mandanten ist jedoch nicht möglich, da die Quarantäneliste Objekte nicht entsprechend der Serverhierarchie anzeigt.

Alarme nach Attributen gruppieren

Die Aggregation von Alarmen hilft bei der Identifizierung von Alarmen, die sich auf denselben Vorfall beziehen können, und vereinfacht so den Untersuchungsprozess.

Um die Funktionalität der Alarm-Aggregation zu aktivieren, müssen Sie Folgendes tun:

- Aktivieren Sie im Hauptmenü den Unterabschnitt **Alarme**.
- Aktivieren Sie den Administrationsserver unter einer Lizenz für Kaspersky Next XDR Optimum und stellen Sie anschließend den Lizenzschlüssel für Kaspersky Next XDR Optimum für Ihre verwalteten Anwendungen bereit.

  Wenn Sie Kaspersky Next XDR Optimum unter einer Demolizenz verwenden, müssen Sie zuerst einen sekundären physischen Administrationsserver hinzufügen und den Server anschließend unter dieser Lizenz aktivieren.

Wenn Sie die Lizenz für Kaspersky Next EDR Optimum verwenden, müssen Sie die Anwendungen, die auf Ihren verwalteten Geräten installiert sind, nicht unter der Lizenz für Kaspersky Next XDR Optimum aktivieren. Sie müssen dies nur für neue Geräte tun, falls vorhanden.
Da die Lizenz für Kaspersky Next XDR Optimum die Mandantenfähigkeit unterstützt, können Sie den Lizenzschlüssel zentral an verwaltete Anwendungen verteilen. Die automatische Verteilung der Lizenz auf sekundäre und virtuelle Administrationsserver wird nicht unterstützt.

Sie können Alarme nach Gerätename, Konto oder Hash-Name (SHA256) aggregieren.

> Alarme werden nur dann nach einem Attribut aggregiert, wenn dieses Attribut nicht leer ist.

Alarme werden aggregiert, wenn sie mindestens ein Attribut gemeinsam haben und innerhalb von 24 Stunden nach einem anderen Alarm in der Gruppe auftreten.

Gehen Sie wie folgt vor, um Alarme nach Attributen zu aggregieren:

1. Gehen Sie im Hauptmenü zu **Überwachung** → **Alarme**.

2. Führen Sie eine der folgenden Aktionen aus:

   - Aktivieren Sie den Umschalter **Aggregation von Alarmen** und wählen Sie dann ein oder mehrere Attribute aus, nach denen Alarme aggregiert werden sollen:

     - **Gerätename**
     - **Benutzerkonto**
     - **Datei-Hash (SHA256)**

     Die Attribute **Gerätename** und **Benutzerkonto** sind standardmäßig ausgewählt.

   - Klicken Sie auf das Einstellungen-Symbol (⚙). Gehen Sie im nächsten Fenster **Tabelleneinstellungen** zur Registerkarte **Gruppierung**. Wählen Sie **ID der Aggregationsgruppe** aus und klicken Sie auf **Übernehmen**.

   Wenn das Aggregieren aktiviert ist, werden die Alarme nach **Ereigniszeitpunkt** vom neuesten zum ältesten sortiert. Zusätzliche Sortieroptionen werden nicht unterstützt. Wenn Sie eine andere Optionsgruppe auswählen, wird das Aggregieren deaktiviert.

In der Tabelle werden die nach Attributen aggregierten Alarme angezeigt. Nicht aggregierte Alarme werden unten in der Tabelle angezeigt.

Jeder Alarm wird nach dem Aggregieren nur einer Gruppe zugewiesen.

Kaspersky Security Center Web Console mit weiteren Kaspersky-Lösungen integrieren

Dieser Abschnitt beschreibt, wie Sie den Zugriff von Kaspersky Security Center Web Console auf andere Kaspersky-Anwendungen, wie Kaspersky Managed Detection and Response, konfigurieren. Außerdem wird in diesem Abschnitt beschrieben, wie der Export in SIEM-Systeme konfiguriert wird.

Hintergrundverbindung herstellen

Zur Konfiguration der Interaktion zwischen Kaspersky Security Center Linux und einer anderen Kaspersky-Anwendung oder -Lösung wie beispielsweise Kaspersky Managed Detection and Response (auch MDR genannt) müssen Sie eine Hintergrundverbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver herstellen. Sie können diese Verbindung nur herstellen, wenn Ihr Konto über die Berechtigung Objekt-ACLs ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** verfügt.

> Sie können die Interaktion nur zwischen Kaspersky Managed Detection and Response und der Windows-basierten Version von Kaspersky Security Center konfigurieren.

So stellen Sie eine Hintergrundverbindung her:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Integration**.
2. Wählen Sie die Registerkarte **Proxyserver-Einstellungen der Web Console**.
3. Stellen Sie im Abschnitt **Integration** den Schalter zum Herstellen einer Hintergrundverbindung auf die Position: **Background-Verbindung für die Integration Aktiviert**.
4. Klicken Sie im folgenden Abschnitt **Background-Verbindung aktivieren** auf die Schaltfläche **OK**.

Die Hintergrundverbindung zwischen Kaspersky Security Center Web Console und dem Administrationsserver wird hergestellt. Der Administrationsserver erstellt für die Hintergrundverbindung ein Benutzerkonto, das als Dienstkonto verwendet wird, um die Interaktion zwischen Kaspersky Security Center Linux und einer anderen Kaspersky-Anwendung aufrechtzuerhalten. Der Name des Dienstkontos enthält den Präfix "NWCSvcUser". Aus Sicherheitsgründen ändert der Administrationsserver das Kennwort des Dienstkontos automatisch alle 30 Tage. Das Dienstkonto kann nicht manuell gelöscht werden. Der Administrationsserver löscht dieses Konto automatisch, wenn Sie die dienstübergreifende Verbindung deaktivieren. Der Administrationsserver erstellt für jede Kaspersky Security Center Web Console und Verwaltungskonsole ein separates Benutzerkonto und weist alle Dienstkonten der Sicherheitsgruppe mit dem Namen "ServiceNwcGroup" zu. Der Administrationsserver erstellt diese Sicherheitsgruppe automatisch während der Installation von Kaspersky Security Center Linux. Diese Sicherheitsgruppe kann nicht manuell gelöscht werden.

Proxyserver-Verbindung konfigurieren

So konfigurieren Sie eine Proxyserver-Verbindung für die Kaspersky Security Center Web Console und die Web-Plug-ins:

1. Gehen Sie im Hauptmenü zu **Einstellungen** → **Integration**.
2. Wählen Sie die Registerkarte **Proxyserver-Einstellungen der Web Console**.
3. Aktivieren Sie bei Option **Proxyserver verwenden**.
4. Geben Sie die Verbindungseinstellungen des Proxyservers an:
   - **Proxyserver-Adresse**
   - **Portnummer**
   - **Authentifizierung am Proxyserver**
   - **Benutzername** (bei aktivierter Option **Am Proxyserver authentifizieren** erforderlich)
   - **Kennwort** (bei aktivierter Option **Am Proxyserver authentifizieren** erforderlich)
5. Klicken Sie auf **Speichern**, um die Verbindungseinstellungen des Proxyservers zu speichern.

Wenn Sie über eine Hierarchie von Administrationsservern verfügen, werden die Verbindungseinstellungen für Proxyserver nicht an Instanzen der Web Console weitergegeben, die sekundäre Administrationsserver verwalten. Sie müssen die Verbindungen mit dem Proxyserver für jede Kaspersky Security Center Web Console separat konfigurieren.

Ferndiagnose der Client-Geräte

Sie können die Ferndiagnose für das Remote-Ausführen der folgenden Vorgänge auf Windows- und Linux-basierten Client-Geräten verwenden:

- Ablaufverfolgung aktivieren und deaktivieren, Ablaufverfolgungsstufe ändern und Ablaufverfolgungsdatei herunterladen
- Herunterladen von Systeminformationen und Programmeinstellungen
- Ereignisprotokolle downloaden
- Erzeugen einer Dump-Datei für eine Anwendung
- Diagnose starten und Diagnoseberichte herunterladen
- Starten, Beenden und Neustart von Programmen

Sie können Ereignisprotokolle und Diagnoseberichte verwenden, die von einem Client-Gerät heruntergeladen wurden, um selbst Probleme zu beheben. Außerdem können Sie bei einer Anfrage an den Technischen Support von Kaspersky von einem Support-Experten aufgefordert werden, Protokolldateien, Dump-Dateien, Ereignisprotokolle und Diagnoseberichte von einem Client-Gerät für eine weitere Analyse bei Kaspersky herunterzuladen.

Öffnen des Fensters für die Ferndiagnose

Um die Ferndiagnose auf Windows- und Linux-basierten Client-Geräten durchzuführen, müssen Sie zunächst das Fenster für die Ferndiagnose öffnen.

So öffnen Sie das Fenster für die Ferndiagnose:

1. Führen Sie einen der folgenden Schritte aus, um das Gerät auszuwählen, für welches Sie das Ferndiagnosefenster öffnen möchten:
   - Wenn das Gerät zu einer Administrationsgruppe gehört, wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.
   - Wenn das Gerät zur Gruppe nicht zugeordneter Geräte gehört, wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Nicht zugeordnete Geräte**.
2. Klicken Sie auf den Namen des gewünschten Geräts.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Erweitert** aus.
4. Klicken Sie auf der Registerkarte **Erweitert** auf **Remote-Diagnose**.

   Dies öffnet das Fenster **Remote-Diagnose** eines Client-Geräts. Wenn zwischen dem Administrationsserver und dem Client-Gerät keine Verbindung hergestellt werden kann, wird eine Fehlermeldung angezeigt.

Wenn Sie alternativ alle Diagnoseinformationen über ein Linux-basiertes Client-Gerät gleichzeitig abrufen möchten, können Sie auf diesem Gerät das Skript collect.sh ausführen.

Aktivieren und Deaktivieren der Ablaufverfolgung für Programme

Sie können die Ablaufverfolgung, einschließlich Xperf-Ablaufverfolgung, aktivieren und deaktivieren.

Ablaufverfolgung aktivieren und deaktivieren

Um die Ablaufverfolgung auf einem Remote-Gerät zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Kaspersky-Anwendungen** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Anwendungen angezeigt.
3. Wählen Sie in der Liste mit Programmen das Programm aus, für welches Sie die Ablaufverfolgung aktivieren oder deaktivieren möchten.

   Die Liste der Optionen zur Ferndiagnose wird geöffnet.
4. Wenn Sie die Ablaufverfolgung aktivieren möchten:

   a. Klicken Sie im Abschnitt **Ablaufverfolgung** auf **Ablaufverfolgung aktivieren**.

   b. Wir empfehlen Ihnen, im nächsten Fenster **Ablaufverfolgungsstufe ändern** die Standardwerte der Einstellungen beizubehalten. Bei Bedarf führt Sie ein Spezialist des Technischen Supports durch den Konfigurationsprozess. Es sind folgende Einstellungen verfügbar:

   - **Ablaufverfolgungsstufe**

     Die Ablaufverfolgungsstufe definiert die Detailstufe der Protokolldatei.

   - **Ablaufverfolgung auf Basis von Rotation**

     Die Anwendung überschreibt die Ablaufverfolgungsinformationen, um eine übermäßige Größenzunahme der Protokolldatei zu vermeiden. Geben Sie die maximale Anzahl von Dateien, die zum Speichern der Ablaufverfolgungsdaten verwendet werden sollen sowie die maximale Größe jeder Datei, an. Wenn die maximale Anzahl von Protokolldateien in maximaler Größe erreicht ist, wird die älteste Protokolldatei gelöscht, damit eine neue Protokolldatei erstellt werden kann.

     Diese Einstellung ist nur für Kaspersky Endpoint Security verfügbar.

   c. Klicken Sie auf die Schaltfläche **Speichern**.

Die Ablaufverfolgung ist für das ausgewählte Programm aktiviert. In einigen Fällen ist es erforderlich, die Sicherheitsanwendungen und deren Aufgabe neu zu starten, um die Ablaufverfolgung zu aktivieren.

Auf Linux-basierten Client-Geräten wird die Ablaufverfolgung der Komponente zum Aktualisieren des Administrationsagenten durch die Einstellungen des Administrationsagenten festgelegt. Daher sind die Optionen **Ablaufverfolgung aktivieren** und **Ablaufverfolgungsstufe ändern** für diese Komponente auf Linux-Client-Geräten deaktiviert.

5. Wenn Sie die Ablaufverfolgung für das ausgewählte Programm deaktivieren möchten, klicken Sie auf die Schaltfläche **Ablaufverfolgung deaktivieren**.

   Die Ablaufverfolgung ist für das ausgewählte Programm deaktiviert.

Aktivieren der Xperf-Ablaufverfolgung

Für Kaspersky Endpoint Security kann ein Spezialist des Technischen Supports Sie dazu auffordern, die Xperf-Ablaufverfolgung zu aktivieren, um Informationen über die Systemleistung zu erhalten.

So aktivieren, deaktivieren und konfigurieren Sie die Xperf-Ablaufverfolgung:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.

2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Kaspersky-Anwendungen** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Anwendungen angezeigt.

3. Wählen Sie in der Liste der Programme das Programm "Kaspersky Endpoint Security für Windows" aus.

   Die Liste mit Optionen zur Ferndiagnose für Kaspersky Endpoint Security für Windows wird angezeigt.

4. Klicken Sie im Abschnitt **Xperf-Ablaufverfolgung** auf **Xperf-Ablaufverfolgung aktivieren**.

   Wenn die Xperf-Ablaufverfolgung bereits aktiviert ist, wird stattdessen die Schaltfläche **Xperf-Ablaufverfolgung deaktivieren** angezeigt. Klicken Sie auf diese Schaltfläche, wenn Sie die Xperf-Ablaufverfolgung für Kaspersky Endpoint Security für Windows deaktivieren möchten.

5. Wählen Sie im nächsten Fenster **Stufe der Xperf-Ablaufverfolgung ändern** eine der folgenden Ablaufverfolgungsstufen entsprechend den Anweisungen des Spezialisten des technischen Supports aus:

   a. Wählen Sie eine der folgenden Ablaufverfolgungsstufen aus:

   - **Leichte Stufe**

     Eine Protokolldatei dieses Typs enthält die Mindestmenge an Informationen über das System.

     Diese Variante ist standardmäßig ausgewählt.

   - **Tiefe Stufe**

     Eine Protokolldatei dieses Typs enthält detailliertere Informationen als Protokolldateien vom Typ *Leicht* und kann von den Experten des Technischen Supports angefordert werden, wenn eine Protokolldatei vom Typ *Leicht* nicht für die Beurteilung der Leistung ausreicht. Die Protokolldatei der Stufe *Tief* enthält technische Informationen zum System einschließlich: Informationen zur Hardware und zum Betriebssystem; Liste der gestarteten und abgeschlossenen Prozesse und Anwendungen; Ereignisse, die für die Leistungsbewertung verwendet wurden; Ereignisse aus dem Windows-Systembewertungstool.

b. Wählen Sie eine der folgenden Xperf-Ablaufverfolgungstypen aus:

- **Basic**

  Die Ablaufverfolgungsinformationen werden während der Ausführung der Sicherheitsanwendung Kaspersky Endpoint Security empfangen.

  Diese Variante ist standardmäßig ausgewählt.

- **Bei Neustart**

  Die Ablaufverfolgungsinformationen werden empfangen, während das Betriebssystem auf dem verwalteten Gerät gestartet wird. Diese Art von Ablaufverfolgung ist wirksam, wenn das Problem, das die Systemleistung beeinträchtigt, nach dem Einschalten des Geräts und vor dem Start von Kaspersky Endpoint Security auftritt.

Sie werden möglicherweise auch aufgefordert, die Option **Größe der Dateien in Rotation, in MB** zu aktivieren, um eine übermäßige Größenzunahme der Protokolldateien zu vermeiden. Geben Sie dann die maximale Größe der Protokolldatei an. Wenn die Datei die maximale Größe erreicht, werden die ältesten Informationen der Ablaufverfolgung durch neue Informationen überschrieben.

c. Legen Sie die Größe der Rotationsdatei fest.

d. Klicken Sie auf die Schaltfläche **Speichern**.

Die Xperf-Ablaufverfolgung ist aktiviert und konfiguriert.

6. Wenn Sie die Xperf-Ablaufverfolgung für Kaspersky Endpoint Security für Windows deaktivieren möchten, klicken Sie im Abschnitt **Xperf-Ablaufverfolgung** auf **Xperf-Ablaufverfolgung deaktivieren**.

   Die Xperf-Ablaufverfolgung ist deaktiviert.

Herunterladen der Protokolldateien eines Programms

Um eine Protokolldatei einer Anwendung herunterzuladen, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Kaspersky-Anwendungen** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme angezeigt.
3. Wählen Sie in der Liste der Programme jenes aus, für das Sie die Protokolldatei herunterladen möchten.
4. Klicken Sie im Abschnitt **Ablaufverfolgung** auf **Protokolldateien**.

   Dadurch wird das Fenster **Ablaufverfolgungsprotokolle des Geräts** geöffnet, welches eine Liste von Protokolldateien anzeigt.
5. Wählen Sie in der Liste der Protokolldateien die Datei aus, die Sie herunterladen möchten.

6. Führen Sie eine der folgenden Aktionen aus:

   - Laden Sie die ausgewählte Datei durch Klicken auf **Herunterladen** herunter. Sie können mehrere Dateien zum Herunterladen auswählen.

   - Um einen Teil der ausgewählten Datei herunterzuladen:

     a. Klicken Sie auf die Schaltfläche **Einen Teil herunterladen**.

        Das gleichzeitige Herunterladen von Teilen mehrerer Dateien ist nicht möglich. Wenn Sie mehr als eine Protokolldatei auswählen, wird die Schaltfläche **Einen Teil herunterladen** deaktiviert.

     b. Geben Sie im folgenden Fenster den Namen und den herunterzuladenden Teil der Datei entsprechend Ihren Anforderungen an.

        Für Linux-basierte Geräte ist das ändern des Namens für Datei-Teile nicht verfügbar.

     c. Klicken Sie auf die Schaltfläche **Herunterladen**.

Die ausgewählte Datei oder deren Teil wird an den von Ihnen angegebenen Speicherort heruntergeladen.

Löschen der Protokolldateien

Sie können nicht mehr benötigte Protokolldateien löschen.

So löschen Sie eine Protokolldatei:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.

2. Wählen Sie im folgenden Ferndiagnosefenster die Registerkarte **Ereignisprotokolle** aus.

3. Klicken Sie im Abschnitt **Protokolldateien** auf die Schaltfläche **Windows Update-Protokolle** oder **Protokolle von Remote-Installation**, je nachdem, welche Protokolldateien Sie löschen möchten.

   > Der Link **Windows Update-Protokolle** ist nur für Windows-basierte Client-Geräte verfügbar.

   Dadurch wird das Fenster **Ablaufverfolgungsprotokolle des Geräts** geöffnet, welches eine Liste von Protokolldateien anzeigt.

4. Wählen Sie in der Liste der Protokolldateien die Dateien aus, die Sie löschen möchten.

5. Klicken Sie auf die Schaltfläche **Entfernen**.

Die ausgewählten Protokolldatei werden gelöscht.

Anwendungseinstellungen herunterladen

Um die Programmeinstellungen von einem Client-Gerät herunterzuladen, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Kaspersky-Anwendungen** aus.
3. Klicken Sie im Abschnitt **Anwendungseinstellungen** auf die Schaltfläche **Herunterladen**, um Informationen über die Einstellungen der auf dem Client-Gerät installierten Anwendungen herunterzuladen.

Das zip-Archiv mit Informationen wird an den angegebenen Speicherort heruntergeladen.

Systeminformationen von einem Client-Gerät herunterladen

So laden Sie Systeminformationen von einem Client-Gerät herunter:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Systeminformationen** aus.
3. Klicken Sie auf die Schaltfläche **Herunterladen**, um die Systeminformationen über das Client-Gerät herunterzuladen.

   Wenn Sie Systeminformationen über ein Linux-basiertes Gerät abrufen, wird der resultierenden Datei eine Dump-Datei für im Notfall beendete Programme hinzugefügt.

   Das Archiv kann vertrauliche Daten (z. B. Schlüssel und Kennwörter) im Klartext enthalten. Es wird empfohlen, die Dateien im Archiv zu überprüfen und solche Daten zu entfernen, bevor Sie das Archiv an den Technischen Support von Kaspersky senden.

Die Datei mit den Informationen wird an den angegebenen Speicherort heruntergeladen.

Ereignisprotokolle downloaden

Um das Ereignisprotokoll von einem Remote-Gerät herunterzuladen, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Klicken Sie im Fenster "Ferndiagnose" auf der Registerkarte **Ereignisprotokolle** auf **Alle Geräteprotokolle**.
3. Wählen Sie im Fenster **Alle Geräteprotokolle** die erforderlichen Protokolle aus.

4. Führen Sie eine der folgenden Aktionen aus:

   - Laden Sie das ausgewählte Protokoll herunter, indem Sie auf **Vollständige Datei herunterladen** klicken.
   - Um einen Teil des ausgewählten Protokolls herunterzuladen:

     a. Klicken Sie auf die Schaltfläche **Einen Teil herunterladen**.

     Das gleichzeitige Herunterladen von Teilen mehrerer Protokolle ist nicht möglich. Wenn Sie mehr als ein Ereignisprotokoll auswählen, wird die Schaltfläche **Einen Teil herunterladen** deaktiviert.

     b. Geben Sie im folgenden Fenster den Namen und den herunterzuladenden Teil des Protokolls entsprechend Ihren Anforderungen an.

     Für Linux-basierte Geräte ist das ändern des Namens für Protokoll-Teile nicht verfügbar.

     c. Klicken Sie auf die Schaltfläche **Herunterladen**.

Das ausgewählte Ereignisprotokoll oder ein Teil davon wird an den angegebenen Speicherort heruntergeladen.

Starten, Stoppen und Neustarten der Anwendung

Sie können Anwendungen auf einem Client-Gerät starten, stoppen und neu starten.

Um eine Anwendung zu starten, zu beenden oder neu zu starten, gehen Sie wie folgt vor:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Kaspersky-Anwendungen** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme angezeigt.
3. Wählen Sie in der Liste der Programme das Programm aus, dass Sie starten, stoppen oder neu starten möchten.
4. Wählen Sie eine Aktion aus, indem Sie auf eine der folgenden Schaltflächen klicken:

   - **Anwendung beenden**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.
   - **Anwendung neu starten**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.
   - **Anwendung starten**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm derzeit nicht ausgeführt wird.

   Je nach ausgewählter Aktion wird das erforderliche Programm auf dem Client-Gerät gestartet, beendet oder neu gestartet.

Wenn Sie den Administrationsagenten neu starten, wird eine Meldung angezeigt, dass die aktuelle Verbindung des Geräts zum Administrationsserver unterbrochen wird.

Remote-Diagnose für den Kaspersky Security Center Linux Administrationsagenten ausführen und Ergebnisse herunterladen

So starten Sie auf einem Remote-Gerät die Diagnose für den Kaspersky Security Center Linux Administrationsagenten und laden die Ergebnisse herunter:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Kaspersky-Anwendungen** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Anwendungen angezeigt.
3. Wählen Sie in der Liste mit den Programmen den **Kaspersky Security Center Linux Administrationsagenten** aus.

   Die Liste der Optionen zur Ferndiagnose wird geöffnet.
4. Klicken Sie im Abschnitt **Diagnosebericht** auf **Diagnose ausführen**.

   Dadurch wird der Ferndiagnoseprozess gestartet und ein Diagnosebericht erstellt. Wenn der Diagnoseprozess abgeschlossen ist, wird die Schaltfläche **Diagnosereport herunterladen** verfügbar.
5. Klicken Sie auf die Schaltfläche **Diagnosereport herunterladen**, um den Bericht herunterzuladen.

Der Bericht wird an den angegebenen Speicherort heruntergeladen.

Ausführen eines Programms auf einem Client-Gerät

Möglicherweise müssen Sie ein Programm auf dem Client-Gerät ausführen, wenn ein Support-Spezialist von Kaspersky Sie dazu auffordert. Sie müssen das Programm nicht auf dem Gerät installieren.

Wenn Sie auf dem Client-Gerät ein benutzerdefiniertes Skript ausführen möchten, können Sie die Umgebungsvariable `KLACDT_SAVE_SETTING` verwenden, um den Pfad zum Speichern der Ausführungsergebnisse zu bestimmen. Beispielsweise:

- Für ein Gerät auf Windows-Basis:

  ```
  @echo some result > %KLACDT_SAVE_SETTING%\res.log
  ```
- Für ein Gerät auf Linux-Basis:

  ```
  echo some result > $KLACDT_SAVE_SETTING/res.log
  ```

Gehen Sie wie folgt vor, um ein Programm auf dem Client-Gerät auszuführen:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Fenster "Ferndiagnose" die Registerkarte **Remote-Ausführung einer Anwendung** aus.

3. Wählen Sie im Feld **Objekttyp** den Objekt-Typ des Objekts, das Sie hochladen möchten:

   - Wählen Sie **Datei**, um die ausführbare Datei hochzuladen.

   - Wählen Sie **Ordner**, um den Ordner mit der Anwendung hochzuladen, die Sie auf dem Client-Gerät ausführen möchten.

     Wenn Sie diesen Objekt-Typ auswählen, wird das Feld **Name der zu startenden ausführbaren Datei** angezeigt. Geben Sie in diesem Feld den Namen der ausführbaren Datei im Ordner an. Sie können auch den relativen Pfad zu der Datei angeben.

   - Wählen Sie **Archiv**, um das zip-Archiv mit der Anwendung hochzuladen, die Sie auf dem Client-Gerät ausführen möchten.

     Wenn Sie diesen Objekt-Typ auswählen, wird das Feld **Name der zu startenden ausführbaren Datei** angezeigt. Geben Sie in diesem Feld den Namen der ausführbaren Datei im Ordner an. Sie können auch den relativen Pfad zu der Datei angeben.

     > Das zip-Archiv muss den Ordner mit dem Tool enthalten. In diesem Ordner befindet sich die ausführbare Datei, die auf einem Remote-Gerät ausgeführt werden soll.

4. Laden Sie das Objekt hoch, indem Sie es im Standard-Dialog des Betriebssystems auswählen oder in das Upload-Feld ziehen.

5. Geben Sie bei Bedarf im Feld **Kommandozeilenargumente** die Befehlszeilenargumente an, die beim Ausführen der ausführbaren Datei übergeben werden sollen.

6. Klicken Sie auf die Schaltfläche **Hochladen und ausführen**, um die angegebene Anwendung auf einem Client-Gerät auszuführen.

7. Nachdem die Anwendung erfolgreich ausgeführt wurde, laden Sie die Ausführungsergebnisse herunter, indem Sie auf die Schaltfläche **Ausführungsergebnisse der Anwendung herunterladen** klicken.

   > Die Ergebnisse einer Anwendungsausführung werden so lange gespeichert, bis Sie eine erneute Diagnose ausführen oder das Fenster schließen.

Die Ferndiagnose eines Client-Geräts mithilfe der Anwendung ist abgeschlossen.

Ferndiagnose auf einem Linux-basierten Client-Gerät ausführen

Kaspersky Security Center Linux ermöglicht es Ihnen, grundlegende Diagnoseinformationen von einem Client-Gerät herunterzuladen. Alternativ können Sie die Diagnoseinformationen über ein Linux-basiertes Gerät mithilfe des Skripts "collect.sh" von Kaspersky abrufen. Dieses Skript wird auf dem zu diagnostizierenden Linux-basierten Client-Gerät ausgeführt und erstellt eine Datei, welche die Diagnoseinformationen, die Systeminformationen für dieses Gerät, die Ablaufverfolgungsdateien der Programme, die Geräteprotokolle und eine Dump-Datei für im Notfall beendete Anwendungen enthält.

Es wird empfohlen, das Skript "collect.sh" zu verwenden, um alle Diagnoseinformationen über das Linux-basierte Client-Gerät auf einmal abzurufen. Wenn Sie die Diagnoseinformationen per Fernzugriff über Kaspersky Security Center Linux herunterladen, müssen Sie alle Abschnitte der Benutzeroberfläche für die Ferndiagnose durchlaufen. Zudem die Diagnoseinformationen für ein Linux-basiertes Gerät werden wahrscheinlich nicht vollständig abgerufen.

Wenn Sie die generierte Datei mit den Diagnoseinformationen an den Technischen Support von Kaspersky senden möchten, löschen Sie alle vertraulichen Informationen, bevor Sie die Datei senden.

Gehen Sie wie folgt vor, um die Diagnoseinformationen mithilfe des Skripts "collect.sh" von einem Linux-basierten Client-Gerät herunterzuladen:

1. Laden Sie das in das Archiv "collect.tar.gz" gepackte Skript "collect.sh" herunter.
2. Kopieren Sie das heruntergeladene Archiv auf das Linux-basierte Client-Gerät, das diagnostiziert werden soll.
3. Führen Sie den folgenden Befehl aus, um das Archiv "collect.tar.gz" zu entpacken:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Führen Sie den folgenden Befehl aus, um die Ausführungsrechte für das Skript anzugeben:

   ```
   # chmod +x collect.sh
   ```

5. Führen Sie das Skript "collect.sh" unter Verwendung eines Kontos mit Administratorrechten aus:

   ```
   # ./collect.sh
   ```

Eine Datei mit den Diagnoseinformationen wird generiert und im Ordner "/tmp/$HOST_NAME-collect.tar.gz" gespeichert.

Drittanbieter-Anwendungen und ausführbare Dateien auf den Client-Geräten verwalten

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center Linux zur Verwaltung von Drittanbieter-Anwendungen und ausführbaren Dateien beschrieben, die auf den Client-Geräten installiert sind.

Programmkontrolle zur Verwaltung ausführbarer Dateien verwenden

Sie können die Programmkontrolle verwenden, um das Starten ausführbarer Dateien auf Benutzergeräten zu erlauben oder blockieren. Die Programmkontrolle unterstützt sowohl Windows- als auch Linux-basierte Betriebssysteme.

Für Linux-basierte Betriebssysteme ist die Komponente "Programmkontrolle" beginnend mit Kaspersky Endpoint Security 11.2 für Linux verfügbar.

Erforderliche Vorrausetzungen

- Kaspersky Security Center Linux ist in Ihrem Unternehmen bereitgestellt.
- Die Richtlinie von Kaspersky Endpoint Security für Linux oder Kaspersky Endpoint Security für Windows wurde erstellt und ist aktiv. Die Programmkontrolle ist in der Richtlinie aktiviert.

Schritte

Die Nutzung der Programmkontrolle erfolgt schrittweise:

1. **Erstellen und Anzeigen der Liste der ausführbaren Dateien auf Client-Geräten**

   Dieser Schritt unterstützt Sie dabei, herauszufinden, welche ausführbaren Dateien sich auf verwalteten Geräten befinden. Öffnen Sie die Liste der ausführbaren Dateien und vergleichen Sie diese mit den Listen der zulässigen und verbotenen ausführbaren Dateien. Die Einschränkungen zur Nutzung ausführbarer Dateien können sich auf die Informationssicherheitsrichtlinien des Unternehmens beziehen.

   Anleitungen: Liste der auf Client-Geräten gespeicherten ausführbaren Dateien abrufen und anzeigen

2. **Erstellen von Kategorien für ausführbare Dateien, die in Ihrem Unternehmen verwendet werden**

   Analysieren Sie die Listen der ausführbaren Dateien, die auf verwalteten Geräten gespeichert sind. Erstellen Sie basierend auf der Analyse Kategorien für ausführbare Dateien. Es wird empfohlen, die Kategorie "Arbeitsanwendung" zu erstellen, welche die Standardauswahl an ausführbaren Dateien enthält, die in Ihrem Unternehmen verwendet werden. Wenn von verschiedenen Sicherheitsgruppen unterschiedliche ausführbare Dateien verwendet werden, können Sie für jede Sicherheitsgruppe eine separate Kategorie erstellen.

Das Starten von ausführbaren Dateien, deren Einstellungen keiner der Regeln der Programmkontrolle entsprechen, wird durch den ausgewählten Betriebsmodus der Komponente geregelt:

- *Deny-Liste*. Dieser Modus wird verwendet, wenn Sie den Start aller ausführbaren Dateien mit Ausnahme jener zulassen möchten, die in den Regeln zum Blockieren angegebenen sind. Dieser Modus ist standardmäßig festgelegt.
- *Allow-Liste*. Dieser Modus wird verwendet, wenn Sie den Start aller ausführbaren Programme mit Ausnahme jener blockieren möchten, die in den Regeln zum Zulassen angegeben sind.

Die Regeln der Programmkontrolle werden durch Kategorien implementiert, denen die ausführbaren Dateien zugeordnet werden. In Kaspersky Security Center Linux gibt es drei Arten von ausführbaren Dateien:

- Manuell zu erweiternde Kategorie. Sie definieren Bedingungen, z. B. Datei-Metadaten, Datei-Hashcode, Dateizertifikat oder Dateipfad, um ausführbare Dateien in die Kategorie aufzunehmen.
- Kategorie für ausführbare Dateien von ausgewählten Geräten. Sie geben ein Gerät an, dessen ausführbare Dateien automatisch in die Kategorie aufgenommen werden.
- Kategorie für ausführbare Dateien aus einem ausgewählten Ordner. Sie geben einen Ordner an, dessen ausführbare Dateien automatisch in die Kategorie aufgenommen werden.

3. **Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security**

   Konfigurieren Sie die Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Linux anhand der Kategorien, die Sie beim vorherigen Schritt erstellt haben.

   Anleitung: Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows

4. **Aktivieren der Komponente "Programmkontrolle" im Test-Modus**

   Um sicherzustellen, dass die Regeln der Programmkontrolle nicht die für die Benutzerarbeit erforderlichen ausführbaren Dateien blockieren, wird empfohlen, das Testen der Regeln der Programmkontrolle zu aktivieren und ihre Funktionsweise nach dem Erstellen neuer Regeln zu analysieren. Wenn das Testen aktiviert ist, blockiert Kaspersky Endpoint Security für Windows keine ausführbaren Dateien, deren Start durch die Regeln der Programmkontrolle unzulässig ist, sondern sendet Benachrichtigungen über deren Start an den Administrationsserver.

   Es wird empfohlen, beim Testen von Regeln der Programmkontrolle die folgenden Aktionen auszuführen:

   - Festlegen des Testzeitraums. Der Testzeitraum kann zwischen mehreren Tagen und zwei Monaten liegen.
   - Untersuchen Sie die Ereignisse, die sich aus dem Testen der Funktionsweise der Programmkontrolle ergeben.

   Anleitung für Kaspersky Security Center Web Console: Konfigurieren der Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Windows. Folgen Sie dieser Anweisung und aktivieren Sie beim Konfigurieren die Option **Testbetrieb**.

5. **Einstellungen der Programmkontrolle ändern**

   Nehmen Sie bei Bedarf Änderungen an den Einstellungen für die Programmkontrolle vor. Auf der Grundlage der Testergebnisse können Sie einer zu erweiternden Kategorie manuell ausführbare Dateien hinzufügen, die sich auf Ereignisse der Programmkontrolle beziehen.

   Anleitung für Kaspersky Security Center Web Console: Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen

6. **Anwenden der Regeln der Programmkontrolle im Funktionsmodus**

   Nachdem die Regeln der Programmkontrolle getestet wurden und die Konfiguration der Kategorien abgeschlossen ist, können Sie die Regeln der Programmkontrolle im Ausführungsmodus anwenden.

   Anleitung für Kaspersky Security Center Web Console: Konfigurieren der Komponente "Programmkontrolle" in der Richtlinie von Kaspersky Endpoint Security für Windows. Folgen Sie dieser Anweisung und deaktivieren Sie beim Konfigurieren die Option **Testbetrieb**.

7. **Überprüfen der Konfiguration der Programmkontrolle**

   Stellen Sie sicher, dass folgende Aktionen ausgeführt wurden:

   - Erstellen von Kategorien für ausführbare Dateien
   - Konfigurieren der Programmkontrolle unter Verwendung der Kategorien
   - Anwenden der Regeln der Programmkontrolle im Funktionsmodus

Ergebnisse

Wenn das Szenario abgeschlossen ist, wird der Start der ausführbaren Dateien auf den verwalteten Geräten gesteuert. Die Benutzer können nur jene ausführbaren Dateien starten, die in Ihrem Unternehmen erlaubt sind. Im Unternehmen verbotene ausführbare Dateien können nicht gestartet werden.

Detaillierte Informationen über die Programmkontrolle finden Sie in der Hilfe für Kaspersky Endpoint Security für Linux und in der Hilfe für Kaspersky Endpoint Security für Windows.

Liste der auf Client-Geräten gespeicherten ausführbaren Dateien abrufen und anzeigen

Sie können die Liste der ausführbaren Dateien, die sich auf den Client-Geräten befinden, auf eine der folgenden Arten abrufen:

- Indem Sie in der Richtlinie von Kaspersky Endpoint Security die Benachrichtigungen über gestartete Anwendungen aktivieren.
- Indem Sie eine Inventarisierungsaufgabe erstellen.

In der Richtlinie von Kaspersky Endpoint Security die Benachrichtigungen über gestartete Anwendungen aktivieren

So aktivieren Sie die Benachrichtigungen über gestartete Anwendungen:

1. Öffnen Sie die Einstellungen der Richtlinie von Kaspersky Endpoint Security und wechseln Sie anschließend zu **Allgemeine Einstellungen → Berichte und Speicher**.
2. Aktivieren Sie in der Einstellungsgruppe **Datenübertragung an den Administrationsserver** das Kontrollkästchen **Über gestartete Anwendungen** und speichern Sie die Änderungen.

   Wenn ein Benutzer versucht, ausführbare Dateien zu starten, werden Informationen über diese Dateien zur Liste der ausführbaren Dateien auf einem Client-Gerät hinzugefügt. Kaspersky Endpoint Security sendet diese Informationen an den Administrationsagenten, welcher sie anschließend an den Administrationsserver weiterleitet.

Eine Inventarisierungsaufgabe erstellen

Für Kaspersky Endpoint Security für Linux ist die Funktion zur Inventarisierung ausführbarer Dateien erst seit Version 11.2 verfügbar.

Sie können die Auslastung der Datenbank verringern und gleichzeitig Informationen über die installierten Anwendungen erhalten. Um Speicherplatz in der Datenbank zu sparen, führen Sie eine Inventarisierungsaufgabe auf Referenzgeräten durch, die mit Ihrem Software-Standardpaket ausgestattet sind. Die empfohlene Anzahl an Geräten beträgt 1-3.

Um eine Inventarisierungsaufgabe für ausführbare Dateien auf den Client-Geräten zu erstellen, gehen Sie folgendermaßen vor:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.

   Die Aufgabenliste wird angezeigt.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Folgen Sie den Schritten des Assistenten.
3. Wählen Sie auf der Seite **Einstellungen der neue Aufgabe** aus der Dropdown-Liste **Anwendung** Kaspersky Endpoint Security für Linux oder Kaspersky Endpoint Security für Windows, in Abhängigkeit des Betriebssystems der Client-Geräte.
4. Wählen Sie in der Dropdown-Liste **Aufgabentyp** die Option **Inventarisierung** aus.
5. Klicken Sie auf der Seite **Erstellung der Aufgabe abschließen** auf **Fertigstellen**.

   Nach Abschluss des Assistenten für das Erstellen einer Aufgabe wird die Aufgabe **Inventarisierung** erstellt und angepasst. Wenn Sie möchten, können Sie die Einstellungen für die erstellte Aufgabe ändern. Daraufhin wird die neu erstellte Aufgabe in der Aufgabenliste angezeigt.

Eine detaillierte Beschreibung der Inventarisierungsaufgabe finden Sie in der Hilfe zu Kaspersky Endpoint Security für Linux und in der Hilfe zu Kaspersky Endpoint Security für Windows.

Nach Ausführung der Aufgabe **Inventarisierung** wird die Liste der auf verwalteten Geräten gespeicherten ausführbaren Dateien erstellt und Sie können die Liste anzeigen.

Im Rahmen einer Inventarisierung können die Dateien folgender Formate erkannt werden (in Abhängigkeit Ihrer gewählten Optionen in den Aufgabeneigenschaften): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR und HTML.

Anzeigen der Liste mit ausführbaren Dateien, die auf verwalteten Geräten gespeichert sind.

Um sich die Liste aller auf den Client-Geräten gespeicherten ausführbaren Dateien anzeigen zu lassen, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **Software-Verwaltung → Drittanbieteranwendungen → Ausführbare Dateien**.

Auf der Seite wird die Liste der auf Client-Geräten gespeicherten ausführbaren Dateien angezeigt.

Bei Bedarf können Sie die ausführbare Datei des verwalteten Geräts an das Gerät senden, auf dem Ihre Kaspersky Security Center Web Console geöffnet ist.

So senden Sie eine ausführbare Datei:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung → Drittanbieteranwendungen → Ausführbare Dateien**.
2. Klicken Sie auf den Link der ausführbaren Datei, die Sie senden möchten.
3. Wechseln Sie im nächsten Fenster zum Abschnitt **Geräte** und aktivieren Sie anschließend das Kontrollkästchen des verwalteten Geräts, von dem Sie die ausführbare Datei senden möchten.

   Stellen Sie vor dem Absenden der ausführbaren Datei durch das Aktivieren des Kontrollkästchens **Verbindung mit Administrationsserver nicht trennen** sicher, dass das verwaltete Gerät eine direkte Verbindung zum Administrationsserver besitzt.

4. Klicken Sie auf die Schaltfläche **Senden**.

   Die ausgewählte ausführbare Datei wird heruntergeladen, um sie anschließend an das Gerät mit Ihrer geöffneten Kaspersky Security Center Web Console weiterzusenden.

Manuell zu erweiternde Programmkategorie erstellen

Sie können einen Satz von Kriterien als Vorlage für ausführbare Dateien angeben, deren Start Sie in Ihrem Unternehmen zulassen oder blockieren möchten. Basierend auf ausführbaren Dateien, die den Kriterien entsprechen, können Sie eine Programmkategorie erstellen und diese in der Konfiguration der Programmkontrolle verwenden.

Um eine manuell zu erweiternde Programmkategorie zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung → Drittanbieteranwendungen → Programmkategorien**.

   Die Seite mit einer Liste der Programmkategorien wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Geben Sie in dem Schritt **Methode zum Erstellen der Kategorie auswählen** den Namen der Programmkategorie ein und wählen Sie die Option **Manuell zu erweiternde Kategorie. Daten über ausführbare Dateien werden manuell zur Kategorie hinzugefügt** aus.

4. Klicken Sie im Schritt **Bedingungen** des Assistenten auf **Hinzufügen**, um ein Bedingungskriterium für das Aufnehmen von Dateien in die Kategorie hinzuzufügen.

5. Gehen Sie im Schritt **Bedingungskriterien** wie folgt vor:

   a. Wählen Sie einen Regeltyp für die Erstellung der Kategorie aus:

   - **Aus der KL-Kategorie**

     Wenn Sie diese Variante wählen, können Sie als Bedingung für die Aufnahme von Anwendungen in eine benutzerdefinierte Kategorie die Kategorie für Kaspersky-Anwendungen angeben. Programme, die zur angegebenen Kaspersky-Kategorie gehören, werden in die benutzerdefinierte Programmkategorie aufgenommen.

   - **Zertifikat aus Datenverwaltung auswählen**

     Wenn Sie diese Option auswählen, können Sie Zertifikate aus der Datenverwaltung angeben. Die Kategoriebedingung entspricht nur den ausführbaren Dateien, die durch das angegebene Zertifikat signiert sind.

     Zertifikate werden zur Datenverwaltung hinzugefügt, wenn Sie eine Inventarisierungsaufgabe erstellt und gestartet haben oder das Kontrollkästchen **Über ausgeführte Anwendungen in der Richtlinie von Kaspersky Endpoint Security** ausgewählt haben. Sie können beide Aktionen ausführen.

     > Informationen über Zertifikate können nur aus ausführbaren Dateien im PE-Format (.exe, .dll, .sys) extrahiert werden.

   - **Pfad der Anwendung festlegen (Masken unterstützt)**

     Wenn diese Option ausgewählt ist, können Sie den Pfad des Ordners auf dem Client-Gerät festlegen, der die ausführbaren Dateien enthält, die zur benutzerdefinierten Programmkategorie hinzugefügt werden sollen.

   - **Wechseldatenträger**

     Wenn Sie diese Variante wählen, können Sie einen Datenträgertyp (beliebiger oder Wechseldatenträger) angeben, auf dem die Anwendung ausgeführt wird. Die auf dem ausgewählten Datenträgertyp ausgeführten Anwendungen werden in die benutzerdefinierte Programmkategorie aufgenommen.

   - **Hash, Metadaten oder Zertifikat**:

     - **Aus Liste der ausführbaren Dateien auswählen**

Wenn Sie diese Variante wählen, können Sie die Anwendungen, die in die Kategorie aufgenommen werden sollen, aus der Liste der ausführbaren Dateien des Client-Geräts auswählen.

- **Aus Programm-Registry auswählen**

  Wenn diese Option ausgewählt ist, wird die Programm-Registry angezeigt. Nachdem Sie eine Anwendung aus der Registrierung ausgewählt haben, öffnet sich ein Fenster mit den ausgefüllten Parametern der Metadaten für die ausgewählte Anwendung:

  - Dateiname.
  - Dateiversion. Sie können den genauen Wert der Version angeben oder eine Bedingung beschreiben, z. B. "größer als 5.0".
  - Name der Anwendung.
  - Version der Anwendung. Sie können den genauen Wert der Version angeben oder eine Bedingung beschreiben, z. B. "größer als 5.0".
  - Hersteller.

  Beachten Sie, dass nur der Start von ausführbaren Dateien, die den angegebenen Parametern entsprechen, blockiert wird, nicht aber der Start der ausgewählten Anwendung. Wenn die Metadaten der ausgewählten Anwendung mit denen der ausführbaren Datei übereinstimmen, die beim Anwendungsstart ausgeführt wird, können Sie mit dem nächsten Schritt fortfahren. Andernfalls müssen Sie die Werte manuell ändern, damit sie mit den Metadaten der ausführbaren Datei übereinstimmen.

- **Manuell angeben**

  Wenn Sie diese Option wählen, müssen Sie als Bedingung für die Aufnahme von Anwendungen in eine benutzerdefinierte Kategorie Datei-Hash, Metadaten oder Zertifikat angeben.

  Datei-Hash

  Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Security Center Linux die Hash-Funktion für die Dateien der Kategorie berechnet. Die Informationen über die von den Hash-Funktionen berechneten Hash-Werte werden in der Datenbank des Administrationsservers gespeichert.

  SHA256 ist eine kryptografische Hash-Funktion, in deren Algorithmen keine Schwachstellen gefunden wurden und die daher momentan als die sicherste kryptographische Funktion angesehen wird. Kaspersky Endpoint Security für Linux unterstützt die SHA256-Berechnung.

  Wählen Sie eine der Optionen zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center Linux aus:

  - Wenn in Ihrem Netzwerk alle installierten Instanzen von Sicherheitsanwendungen aus Kaspersky Endpoint Security für Linux bestehen, aktivieren Sie das Kontrollkästchen **SHA256**.
  - Aktivieren Sie das Kontrollkästchen **MD5-Hash** nur dann, wenn Sie Kaspersky Endpoint Security für Windows verwenden. Die MD5-Hash-Funktion wird von Kaspersky Endpoint Security für Linux nicht unterstützt.

  Metadaten

  Wenn diese Option ausgewählt ist, können Sie Dateimetadaten als Dateinamen, Dateiversion und Hersteller angeben. Die Kategoriebedingung entspricht nur den ausführbaren Dateien mit denselben Metadaten.

  Zertifikat

Wenn Sie diese Option auswählen, können Sie Zertifikate aus der Datenverwaltung angeben. Die Kategoriebedingung entspricht nur den ausführbaren Dateien, die durch das angegebene Zertifikat signiert sind.

Zertifikate werden zur Datenverwaltung hinzugefügt, wenn Sie eine Inventarisierungsaufgabe erstellt und gestartet haben oder das Kontrollkästchen **Über ausgeführte Anwendungen in der Richtlinie von Kaspersky Endpoint Security** ausgewählt haben. Sie können beide Aktionen ausführen.

- **Aus archiviertem Ordner**

  Wenn diese Option ausgewählt ist, können Sie eine Datei eines archivierten Ordners angeben und dann auswählen, welche Bedingung Sie verwenden möchten, um Anwendungen zu der Benutzerkategorie hinzuzufügen. Der archivierte Ordner wird entpackt und die von Ihnen ausgewählten Bedingungen werden auf die Dateien in diesem Ordner angewendet. Sie können eine der folgenden Kriterien als Bedingung auswählen:

  - **Datei-Hash**

    Sie wählen aus, mit welcher Hash-Funktion (MD5 oder SHA256) die Hash-Werte berechnet werden sollen. Anwendungen, die denselben Hash-Wert haben wie die Dateien in dem archivierten Ordner, werden in die benutzerdefinierte Programmkategorie aufgenommen.

    Wählen Sie eine MD5-Hash-Funktion nur dann, wenn Sie Kaspersky Endpoint Security für Windows verwenden. Die MD5-Hash-Funktion wird von Kaspersky Endpoint Security für Linux nicht unterstützt.

  - **Metadaten**

    Sie wählen aus, welche Metadaten Sie als Kriterien verwenden möchten. Ausführbare Dateien mit denselben Metadaten werden in die benutzerdefinierte Programmkategorie aufgenommen.

  - **Zertifikat**

    Sie wählen aus, welche Zertifikatseigenschaften (Zertifikatssubjekt, Fingerabdruck oder Aussteller) Sie als Kriterien verwenden möchten. Ausführbare Dateien, die mit dem Zertifikat signiert sind, das identische Eigenschaften hat, werden zur Benutzerkategorie hinzugefügt.

  Die Kriterien **Metadaten** und **Zertifikat** müssen nach dem Hochladen einer Datei oder eines archivierten Ordners manuell eingegeben werden, wenn Sie diese Kriterien verwenden möchten.

  Wenn diese Option ausgewählt ist, können Sie eine Datei eines archivierten Ordners angeben und dann auswählen, welche Bedingung Sie verwenden möchten, um Anwendungen zu der Benutzerkategorie hinzuzufügen. Der archivierte Ordner wird entpackt und die von Ihnen ausgewählten Bedingungen werden auf die Dateien in diesem Ordner angewendet. Sie können eine der folgenden Kriterien als Bedingung auswählen:

  - **Datei-Hash**

    Sie wählen aus, mit welcher Hash-Funktion (MD5 oder SHA256) die Hash-Werte berechnet werden sollen. Anwendungen, die denselben Hash-Wert haben wie die Dateien in dem archivierten Ordner, werden in die benutzerdefinierte Programmkategorie aufgenommen.

    Wählen Sie eine MD5-Hash-Funktion nur dann, wenn Sie Kaspersky Endpoint Security für Windows verwenden. Die MD5-Hash-Funktion wird von Kaspersky Endpoint Security für Linux nicht unterstützt.

  - **Metadaten**

    Sie wählen aus, welche Metadaten Sie als Kriterien verwenden möchten. Ausführbare Dateien mit denselben Metadaten werden in die benutzerdefinierte Programmkategorie aufgenommen.

- **Zertifikat**

  Sie wählen aus, welche Zertifikatseigenschaften (Zertifikatssubjekt, Fingerabdruck oder Aussteller) Sie als Kriterien verwenden möchten. Ausführbare Dateien, die mit dem Zertifikat signiert sind, das identische Eigenschaften hat, werden zur Benutzerkategorie hinzugefügt.

Die Kriterien **Metadaten** und **Zertifikat** müssen nach dem Hochladen einer Datei oder eines archivierten Ordners manuell eingegeben werden, wenn Sie diese Kriterien verwenden möchten.

b. Fügen Sie bei Bedarf einen Kommentar in das Feld **Beschreibung** ein. Sie können maximal 1000 Zeichen eingeben.

Sie können den Kommentar später ändern oder löschen, indem Sie in den Eigenschaften der Programmkategorie auf die Registerkarte **Bedingungen** klicken und anschließend in der Spalte **Kriterium der Bedingung** den Link mit der Bedingung anklicken, für welche Sie den Kommentar ändern oder löschen möchten.

Wenn Sie den Regeltyp **Aus der KL-Kategorie** auswählen, können Sie einen Kommentar für alle Bedingungen hinzufügen, die basierend auf diesem Regeltyp erstellt werden sollen. Sie können den Kommentar für jede Bedingung separat bearbeiten oder löschen.

Das ausgewählte Kriterium wird zur Liste mit Kriterien hinzugefügt.

Sie können der zu erstellenden Programmkategorie beliebig viele Kriterien hinzufügen.

6. Klicken Sie in dem Schritt **Ausschlüsse** des Assistenten auf **Hinzufügen**, um ein exklusives Bedingungskriterium hinzufügen, nach dem Dateien aus der gerade erstellten Kategorie ausgeschlossen werden sollen.

   Bei Bedarf können Sie in dem Feld **Beschreibung** einen Kommentar hinzufügen. Sie können maximal 1000 Zeichen eingeben.

   Sie können den Kommentar später ändern oder löschen, indem Sie in den Eigenschaften der Programmkategorie auf die Registerkarte **Ausschlüsse** klicken und anschließend in der Spalte **Kriterium der Bedingung** den Link mit der Bedingung anklicken, für welche Sie den Kommentar ändern oder löschen möchten.

7. Wählen Sie im Schritt **Bedingungskriterien** einen Regeltyp aus der Liste aus, so wie Sie einen Regeltyp zum Erstellen einer Kategorie ausgewählt haben.

Nach Abschluss des Assistenten wird die Programmkategorie erstellt und in der Liste der Programmkategorien angezeigt. Sie können die erstellte Programmkategorie verwenden, wenn Sie die "Programmkontrolle" anpassen.

Detaillierte Informationen über die Programmkontrolle finden Sie in der Hilfe für Kaspersky Endpoint Security für Linux und in der Hilfe für Kaspersky Security für Windows.

Programmkategorie mit ausführbaren Dateien von ausgewählten Geräten erstellen

Sie können ausführbare Dateien von ausgewählten Geräten als Vorlage für ausführbare Dateien verwenden, die Sie zulassen oder blockieren möchten. Basierend auf ausführbaren Dateien von ausgewählten Geräten können Sie eine Programmkategorie erstellen und diese in der Konfiguration der Programmkontrolle verwenden.

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die Komponente "Programmkontrolle" ist in der Richtlinie von Kaspersky Endpoint Security aktiviert.
- Eine wurde Liste mit den ausführbaren Dateien, die sich auf den verwalteten Geräten befinden, abgerufen.

Um eine Programmkategorie zu erstellen, die ausführbare Dateien von ausgewählten Geräten enthält, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Programmkategorien**.

   Die Seite mit der Liste der Kategorien ausführbarer Dateien wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

3. Geben Sie im Schritt **Methode zum Erstellen der Kategorie auswählen** den Kategorienamen ein und wählen Sie die Option **Kategorie für ausführbare Dateien von ausgewählten Geräten. Diese ausführbaren Dateien werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt**.

4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

5. Wählen Sie im folgenden Fenster ein Gerät oder mehrere Geräte aus, deren ausführbare Dateien zum Erstellen der Programmkategorie verwendet werden sollen.

6. Geben Sie die folgenden Einstellungen an:

   - **Algorithmus für die Berechnung der Hash-Funktion**

     Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Security Center Linux die Hash-Funktion für die Dateien der Kategorie berechnet. Die Informationen über die von den Hash-Funktionen berechneten Hash-Werte werden in der Datenbank des Administrationsservers gespeichert.

     SHA256 ist eine kryptografische Hash-Funktion, in deren Algorithmen keine Schwachstellen gefunden wurden und die daher momentan als die sicherste kryptographische Funktion angesehen wird. Kaspersky Endpoint Security für Linux unterstützt die SHA256-Berechnung.

     Wählen Sie eine der Optionen zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center Linux aus:

     - Wenn in Ihrem Netzwerk alle installierten Instanzen von Sicherheitsanwendungen aus Kaspersky Endpoint Security für Linux bestehen, aktivieren Sie das Kontrollkästchen **SHA256**.

     Aktivieren Sie das Kontrollkästchen **MD5-Hash** nur dann, wenn Sie Kaspersky Endpoint Security für Windows verwenden. Die MD5-Hash-Funktion wird von Kaspersky Endpoint Security für Linux nicht unterstützt.

     Standardmäßig ist das Kontrollkästchen **SHA256 für die Dateien der Kategorie berechnen (unterstützt für Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher)** aktiviert.

     Standardmäßig ist das Kontrollkästchen **MD5 für die Dateien der Kategorie berechnen (unterstützt für Vorgängerversionen von Kaspersky Endpoint Security 10 Service Pack 2 für Windows)** deaktiviert.

   - **Daten mit der Datenverwaltung des Administrationsservers synchronisieren**

     Wählen Sie diese Option, wenn der Administrationsserver die Änderungen in dem bzw. den angegebenen Ordner(n) regelmäßig überprüfen soll.

     Diese Option ist standardmäßig deaktiviert.

Wenn Sie diese Option aktivieren, geben Sie den Zeitraum (in Stunden) an, in dem die Änderungen in den angegebenen Ordnern überprüft werden sollen. Standardmäßig beträgt das Untersuchungsintervall 24 Stunden.

- **Dateityp**

  In diesem Abschnitt können Sie den Dateityp angeben, mit dem die Programmkategorie erstellt wird.

  Alle Dateien. Alle Dateien werden beim Erstellen der Kategorie berücksichtigt. Diese Variante ist standardmäßig ausgewählt.

  Nur Dateien, die keiner Programmkategorie entsprechen. Nur Dateien außerhalb der Programmkategorien werden beim Erstellen der Kategorie berücksichtigt.

- **Ordner**

  In diesem Abschnitt können Sie Ordner auf dem ausgewählten Gerät (bzw. den ausgewählten Geräten) angeben, die Dateien enthalten, mit denen die Programmkategorie erstellt wird.

  Alle Ordner. Alle Ordner werden beim Erstellen der Kategorie berücksichtigt. Diese Variante ist standardmäßig ausgewählt.

  Angegebener Ordner. Nur der angegebene Ordner wird beim Erstellen der Kategorie berücksichtigt. Bei Auswahl dieser Option müssen Sie den Pfad zum Ordner angeben.

Nach Abschluss des Assistenten wird die Kategorie der ausführbaren Dateien erstellt. Sie wird in der Liste der Kategorien angezeigt. Sie können die erstellte Kategorie verwenden, wenn Sie die Programmkontrolle konfigurieren.

Erstellen einer Programmkategorie mit ausführbaren Dateien aus einem ausgewählten Ordner

Sie können die ausführbaren Dateien aus einem bestimmten Ordner als Standard für die ausführbaren Dateien verwenden, die Sie in Ihrem Unternehmen zulassen oder blockieren möchten. Basierend auf den ausführbaren Dateien aus dem ausgewählten Ordner können Sie eine Programmkategorie erstellen und diese verwenden, um die Komponente "Programmkontrolle" anzupassen.

Um eine Kategorie zu erstellen, die ausführbare Dateien aus dem ausgewählten Ordner enthält:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Programmkategorien**.

   Die Seite mit der Liste an Kategorien wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

3. Geben Sie im Schritt **Methode zum Erstellen der Kategorie auswählen** den Kategorienamen ein und wählen Sie die Option **Kategorie für ausführbare Dateien aus einem bestimmten Ordner. Ausführbare Dateien von Anwendungen, die sich in dem angegebenen Ordner befinden, werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt** aus.

4. Geben Sie den Ordner an, dessen ausführbare Dateien zum Erstellen der Kategorie verwendet werden.

5. Passen Sie die folgenden Einstellungen an:

- **Dynamic Link Libraries (.dll) in diese Kategorie aufnehmen**

  Zur Programmkategorie werden dynamisch verbundene Bibliotheken (dll-Dateien) hinzugefügt und die Komponente "Programmkontrolle" registriert die Aktionen solcher Bibliotheken, die im System gestartet werden. Es ist möglich, dass nach der Aufnahme von dll-Dateien in die Kategorie die Leistung von Kaspersky Security Center sinkt.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Skriptdateien in diese Kategorie aufnehmen**

  Zur Programmkategorie werden Informationen zu Skripten hinzugefügt und die Skripte werden von der Komponente "Schutz vor Web-Bedrohungen" nicht gesperrt. Es ist möglich, dass nach der Aufnahme von Daten zu Skripten in die Kategorie die Leistung von Kaspersky Security Center sinkt.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Algorithmus für die Berechnung der Hash-Funktion**: **SHA256 für Dateien in dieser Kategorie berechnen (unterstützt ab Kaspersky Endpoint Security 10 Service Pack 2 für Windows) / MD5 für Dateien in dieser Kategorie berechnen (unterstützt bis Kaspersky Endpoint Security 10 Service Pack 2 für Windows)**

  Je nach Version der Sicherheitsanwendung, die auf den Geräten in Ihrem Netzwerk installiert ist, müssen Sie einen Algorithmus auswählen, mit dem Kaspersky Security Center Linux die Hash-Funktion für die Dateien der Kategorie berechnet. Die Informationen über die von den Hash-Funktionen berechneten Hash-Werte werden in der Datenbank des Administrationsservers gespeichert.

  SHA256 ist eine kryptografische Hash-Funktion, in deren Algorithmen keine Schwachstellen gefunden wurden und die daher momentan als die sicherste kryptographische Funktion angesehen wird. Kaspersky Endpoint Security für Linux unterstützt die SHA256-Berechnung.

  Wählen Sie eine der Optionen zur Berechnung der Hash-Funktion für die Dateien der Kategorie durch Kaspersky Security Center Linux aus:

  - Wenn in Ihrem Netzwerk alle installierten Instanzen von Sicherheitsanwendungen aus Kaspersky Endpoint Security für Linux bestehen, aktivieren Sie das Kontrollkästchen **SHA256**.

  Aktivieren Sie das Kontrollkästchen **MD5-Hash** nur dann, wenn Sie Kaspersky Endpoint Security für Windows verwenden. Die MD5-Hash-Funktion wird von Kaspersky Endpoint Security für Linux nicht unterstützt.

  Standardmäßig ist das Kontrollkästchen **SHA256 für die Dateien der Kategorie berechnen (unterstützt für Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher)** aktiviert.

  Standardmäßig ist das Kontrollkästchen **MD5 für die Dateien der Kategorie berechnen (unterstützt für Vorgängerversionen von Kaspersky Endpoint Security 10 Service Pack 2 für Windows)** deaktiviert.

- **Untersuchung des Ordners auf Änderungen erzwingen**

  Wenn diese Option aktiviert ist, erzwingt das Programm regelmäßig eine Prüfung des Ordners für die Erweiterung von Kategorien auf Veränderungen. Das Prüfintervall in Stunden kann im Eingabefeld neben dem Kontrollkästchen eingegeben werden. Standardmäßig beträgt das Intervall für die erzwungene Prüfung 24 Stunden.

  Ist diese Option deaktiviert, erfolgt keine erzwungene Prüfung des Ordners. Der Server greift auf die Dateien im Ordner zu, wenn diese verändert, hinzugefügt oder gelöscht werden.

  Diese Option ist standardmäßig deaktiviert.

Nach Abschluss des Assistenten wird die Kategorie der ausführbaren Dateien erstellt. Sie wird in der Liste der Kategorien angezeigt. Sie können die Kategorie in der Konfiguration der Programmkontrolle verwenden.

Detaillierte Informationen über die Programmkontrolle finden Sie in der Hilfe für Kaspersky Endpoint Security für Linux und in der Hilfe für Kaspersky Security für Windows.

Liste der Programmkategorien anzeigen

Sie können die Liste der konfigurierten Kategorien für die ausführbaren Dateien und die Einstellungen der einzelnen Kategorien anzeigen.

Um die Liste der Programmkategorien anzuzeigen,

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Programmkategorien**.

Die Seite mit der Liste an Kategorien wird angezeigt.

Um die Eigenschaften einer Programmkategorie anzuzeigen,

Klicken Sie auf den Namen der Kategorie.

Das Eigenschaftenfenster der Kategorie wird angezeigt. Die Eigenschaften sind auf mehreren Registerkarten angeordnet.

Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen

Nachdem Sie die "Programmkontrolle" in den Richtlinien von Kaspersky Endpoint Security angepasst haben, werden in der Ereignisliste die folgenden Ereignisse angezeigt:

- **Anwendungsstart verboten** (*kritisches* Ereignis). Dieses Ereignis wird angezeigt, wenn Sie die Programmkontrolle so konfiguriert haben, dass Regeln angewendet werden.
- **Der Start der Anwendung ist im Testbetrieb untersagt** (*Infomeldungsereignis*). Dieses Ereignis wird angezeigt, wenn Sie die Programmkontrolle so konfiguriert haben, dass Regeln getestet werden.
- **Nachricht an den Administrator über verbotene Anwendungsstarts** (Ereignistyp *Warnung*). Dieses Ereignis wird angezeigt, wenn Sie in der "Programmkontrolle" das Anwenden von Regeln festgelegt haben, und ein Benutzer auf eine Anwendung zugreifen möchte, das beim Start blockiert wurde.

Es wird empfohlen, Ereignisauswahlen zu erstellen, um Ereignisse anzuzeigen, die sich auf den Betrieb der Programmkontrolle beziehen.

Sie können ausführbare Dateien, die sich auf Ereignisse der Programmkontrolle beziehen, zu einer vorhandenen Programmkategorie oder zu einer neuen Programmkategorie hinzufügen. Das Hinzufügen ausführbarer Dateien ist jedoch nur bei einer manuell zu erweiternden Programmkategorie möglich.

Um ausführbare Dateien, die sich auf Ereignisse der Programmkontrolle beziehen, zu einer Programmkategorie hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung → Ereignisauswahlen**.

   Die Liste der Ereignisauswahlen wird angezeigt.

2. Wählen Sie die Ereignisauswahl aus, um Ereignisse im Zusammenhang mit der Programmkontrolle anzuzeigen und diese Ereignisauswahl zu starten.

   Wenn Sie keine Ereignisauswahl für die Programmkontrolle erstellt haben, können Sie eine vordefinierte Auswahl auswählen und starten, z. B. **Letzte Ereignisse**.

   Die Liste der Ereignisse wird angezeigt.

3. Wählen Sie die Ereignisse aus, für die Sie ausführbare Dateien der Programmkategorie hinzufügen möchten, und klicken Sie auf **Einer Kategorie zuweisen**.

   Der Assistent für das Erstellen einer Kategorie wird gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

4. Legen Sie auf der Seite des Assistenten die relevanten Einstellungen fest:

   - Wählen Sie im Abschnitt **Aktion mit der Datei, die das Ereignis auslöste** eine der folgenden Optionen aus:

     - **Zu neuer Programmkategorie hinzufügen**

       Wählen Sie diese Option, wenn Sie eine neue Programmkategorie basierend auf ereignisbezogenen ausführbaren Dateien erstellen möchten.

       Diese Variante ist standardmäßig ausgewählt.

       Wenn Sie diese Option ausgewählt haben, geben Sie einen neuen Kategorienamen an.

     - **Zu bestehender Programmkategorie hinzufügen**

       Wählen Sie diese Option, wenn Sie in einer bestehenden Programmkategorie ereignisbezogene ausführbare Dateien hinzufügen möchten.

       Diese Variante ist standardmäßig nicht ausgewählt.

       Wenn Sie diese Option ausgewählt haben, wählen Sie die Programmkategorie mit manuell hinzugefügtem Inhalt aus, zu der Sie ausführbare Dateien hinzufügen möchten.

   - Wählen Sie im Abschnitt **Regeltyp** eine der folgenden Optionen aus:

     - **Regeln zum Hinzufügen zu den Einschlüssen**

     - **Regeln zum Hinzufügen zu den Ausschlüssen**

   - Wählen Sie im Abschnitt **Als Bedingung verwendete Parameter** eine der folgenden Optionen aus:

     - **Zertifikatinformationen (oder SHA256-Hashes für Dateien ohne Zertifikat)**

       Die Dateien können vom Zertifikat signiert werden. Dabei können von einem Zertifikat mehrere Dateien signiert werden. Beispielsweise können verschiedene Versionen einer Anwendung von einem Zertifikat signiert sein oder mehrere verschiedene Anwendungen eines Herstellers können von einem Zertifikat signiert sein. Bei der Wahl des Zertifikates können mehrere Anwendungsversionen oder mehrere Anwendungen eines Herstellers in der Kategorie vorhanden sein.

       Jede Datei hat ihre eindeutige SHA256-Hash-Funktion. Bei der Auswahl der SHA256-Hash-Funktion enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Anwendungsversion.

Wählen Sie diese Variante, wenn Sie die die Zertifikatsdetails einer ausführbaren Datei (oder die SHA256-Hash-Funktion für Dateien ohne Zertifikat) zu den Regeln der Kategorie hinzufügen möchten.

Diese Variante ist standardmäßig ausgewählt.

- **Zertifikatinformationen (Dateien ohne Zertifikat werden übersprungen)**

  Die Dateien können vom Zertifikat signiert werden. Dabei können von einem Zertifikat mehrere Dateien signiert werden. Beispielsweise können verschiedene Versionen einer Anwendung von einem Zertifikat signiert sein oder mehrere verschiedene Anwendungen eines Herstellers können von einem Zertifikat signiert sein. Bei der Wahl des Zertifikates können mehrere Programmversionen oder mehrere Programme eines Herstellers in der Kategorie vorhanden sein.

  Wählen Sie diese Variante, wenn Sie die Zertifikatsdaten einer ausführbaren Datei zu den Regeln der Kategorie hinzufügen möchten. Wenn die ausführbare Datei kein Zertifikat hat, wird eine solche Datei übersprungen. Die entsprechenden Informationen werden nicht zur Kategorie hinzugefügt.

- **Nur SHA256 (Dateien ohne Hash werden übersprungen)**

  Jede Datei hat ihre eindeutige SHA256-Hash-Funktion. Bei der Auswahl der SHA256-Hash-Funktion enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Programmversion.

  Wählen Sie diese Variante, wenn Sie nur die Daten der SHA256-Hash-Funktion einer ausführbaren Datei zu den Regeln der Kategorie hinzufügen möchten

- **Nur MD5 (Modus eingestellt. Nur für Kaspersky Endpoint Security 10 Service Pack 1)**

  Wählen Sie diese Option nur aus, wenn Sie Kaspersky Endpoint Security für Windows verwenden. Eine MD5-Hash-Funktion wird von Kaspersky Endpoint Security für Linux nicht unterstützt.

  Jede Datei hat ihre eindeutige MD5 Hash-Funktion. Bei der Auswahl der MD5 Hash-Funktion enthält die Kategorie nur die entsprechende Datei, beispielsweise die angegebene Anwendungsversion.

5. Klicken Sie auf die Schaltfläche **OK**.

   Nach Abschluss des Assistenten werden ausführbare Dateien, die sich auf Ereignisse der Programmkontrolle beziehen, zu der vorhandenen Programmkategorie oder zu einer neuen Programmkategorie hinzugefügt. Sie können die Einstellungen der Programmkategorie anzeigen, die Sie geändert oder erstellt haben.

Detaillierte Informationen über die Programmkontrolle finden Sie in der Hilfe für Kaspersky Endpoint Security für Linux und in der Hilfe für Kaspersky Security für Windows.

Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows konfigurieren

Nachdem Sie die Kategorien der "Programmkontrolle" erstellt haben, können Sie diese verwenden, um die "Programmkontrolle" in den Richtlinien von Kaspersky Endpoint Security für Windows anzupassen.

So konfigurieren Sie die Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows:

1. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

   Eine Seite mit einer Liste der Richtlinien wird angezeigt.

2. Klicken Sie auf die Richtlinie **Kaspersky Endpoint Security für Windows**.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.

3. Wechseln Sie zu **Anwendungseinstellungen → Sicherheitskontrollen → Programmkontrolle**.

   Das Fenster **Programmkontrolle** mit den entsprechenden Eigenschaften wird angezeigt.

4. Die Option **Programmkontrolle** ist standardmäßig aktiviert. Setzen Sie den Umschalter auf **Programmkontrolle DEAKTIVIERT**, um die Option zu deaktivieren.

5. Aktiveren Sie in den Sperreinstellungen der **Einstellungen der Programmkontrolle** den Ausführungsmodus, um die Regeln der Programmkontrolle anzuwenden und Kaspersky Endpoint Security für Windows zu erlauben, den Start von Anwendungen zu blockieren.

   Wenn Sie die Regeln der Programmkontrolle testen möchten, können Sie in den **Einstellungen der Programmkontrolle** den Testmodus aktivieren. Im Testmodus blockiert Kaspersky Endpoint Security für Windows den Start von Anwendungen nicht, sondern protokolliert Informationen über ausgelöste Regeln im Bericht. Klicken Sie auf den Link **Bericht anzeigen**, um diese Informationen anzuzeigen.

6. Aktivieren Sie die Option **Laden von DDL-Modulen überwachen**, wenn Kaspersky Endpoint Security für Windows beim Starten von Anwendungen das Laden von DLL-Modulen überwachen soll.

   Informationen über das Modul und die Anwendung, die das Modul geladen hat, werden in einem Bericht gespeichert.

   Kaspersky Endpoint Security für Windows überwacht nur die DLL-Module und -Treiber, die nach der Auswahl der Option **Laden von DDL-Modulen überwachen** geladen wurden. Starten Sie das Gerät nach Auswahl der Option **Laden von DLL-Modulen überwachen** neu, wenn Kaspersky Endpoint Security für Windows alle DLL-Module und -Treiber überwachen soll. Dies betrifft auch jene, die vor dem Start von Kaspersky Endpoint Security für Windows geladenen werden.

7. (Optional) Ändern Sie im Block **Nachrichtenvorlagen** die Vorlage der Nachricht, die bei einer Blockierung eines Anwendungsstarts angezeigt wird, sowie die Vorlage der E-Mail, die an Sie gesendet wird.

8. Wählen Sie im Einstellungsblock **Modus der Programmkontrolle** den Modus **Deny-Liste** oder **Allow-Liste** aus.

   Der Modus **Deny-Liste** ist standardmäßig ausgewählt.

9. Klicken Sie auf den Link **Einstellungen für Regellisten**.

   Das Fenster **Deny-Listen und Allow-Listen** wird geöffnet. Dort können Sie eine Programmkategorie hinzufügen. Standardmäßig ist die Registerkarte **Deny-Liste** ausgewählt, wenn der Modus **Deny-Liste** ausgewählt ist, bzw. die Registerkarte **Allow-Liste**, wenn der Modus **Allow-Liste** ausgewählt ist.

10. Klicken Sie im Fenster **Deny-Listen und Allow-Listen** auf **Hinzufügen**.

    Das Fenster **Regel der Programmkontrolle** wird geöffnet.

11. Klicken Sie auf den Link **Bitte wählen Sie eine Kategorie**.

    Das Fenster **Programmkategorie** wird geöffnet.

12. Fügen Sie die zuvor erstellte Programmkategorie(n) hinzu.

    Klicken Sie auf **Bearbeiten**, um die Einstellungen einer erstellten Kategorie zu bearbeiten.

    Klicken Sie auf **Hinzufügen**, um eine neue Kategorie zu erstellen.

    Klicken Sie auf **Löschen**, um eine Kategorie aus der Liste zu löschen.

13. Nachdem Sie die Liste der Programmkategorien erstellt haben, klicken Sie auf **OK**.

    Das Fenster **Programmkategorie** wird geschlossen.

14. Erstellen Sie im Fenster der Regel der **Programmkontrolle** im Abschnitt **Subjekte und deren Rechte** eine Liste der Benutzer und Benutzergruppen, für welche die Regel der Programmkontrolle gelten soll.

15. Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Fenster **Regel der Programmkontrolle** zu schließen.

16. Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Fenster **Deny-Listen und Allow-Listen** zu schließen.

17. Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Fenster **Programmkontrolle** zu schließen.

18. Schließen Sie das Fenster mit den Richtlinieneinstellungen für Kaspersky Endpoint Security für Windows.

    Die Programmkontrolle wird konfiguriert. Nachdem die Richtlinie an die Client-Geräte verteilt wurde, wird der Start der ausführbaren Dateien verwaltet.

Detaillierte Informationen über die Programmkontrolle finden Sie in der Hilfe für Kaspersky Endpoint Security für Linux und in der Hilfe für Kaspersky Security für Windows.

Liste der auf Client-Geräten installierten Programme abrufen und anzeigen

Kaspersky Security Center Linux führt eine Inventarisierung der Software durch, die auf den verwalteten Client-Geräten unter Linux und Windows installiert ist.

Der Administrationsagent erstellt eine Liste der auf dem Gerät installierten Anwendungen und leitet die Liste an den Administrationsserver weiter. Es dauert etwa 10-15 Minuten, bis der Administrationsagent die Anwendungsliste aktualisiert hat.

Bei Windows-basierten Client-Geräten erhält der Administrationsagent die meisten Informationen über installierte Anwendungen aus der Windows-Registrierung. Bei Linux-basierten Client-Geräten werden dem Administrationsagenten die Informationen über installierte Anwendungen durch die Paketmanager bereitgestellt.

Um die Liste mit auf verwalteten Geräten installierten Anwendungen anzuzeigen, gehen Sie wie folgt vor:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Drittanbieteranwendungen** → **Programm-Registry**.

   Die Seite zeigt eine Tabelle mit den Anwendungen an, die auf verwalteten Geräten installiert sind. Wählen Sie eine Anwendung aus, um seine Eigenschaften anzeigen, z. B. Name des Anbieters, Versionsnummer, Liste der ausführbaren Dateien, Liste der Geräte mit der installierten Anwendung.

2. Sie können die Daten der Tabelle mit installierten Anwendungen wie folgt gruppieren und filtern:

   - Klicken Sie auf das Einstellungen-Symbol ( ) in der oberen rechten Ecke der Tabelle.

     Wählen Sie im geöffneten Menü **Spalten-Einstellungen** die Spalten aus, die in der Tabelle angezeigt werden sollen. Um den Betriebssystemtyp der Client-Geräte anzuzeigen, auf denen die Anwendung installiert ist, wählen Sie die Spalte **Typ des Betriebssystems** aus.

   - Klicken Sie auf das Filter-Symbol ( ) in der oberen rechten Ecke der Tabelle, geben Sie anschließend das Filterkriterium im aufgerufenen Menü an und wenden Sie es an.

     Die gefilterte Tabelle der installierten Anwendungen wird angezeigt.

So zeigen Sie eine Liste der Anwendungen an, die auf bestimmten verwalteten Geräten installiert sind:

Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)** → **<Gerätename>** → **Erweitert** → **Programm-Registry**. In diesem Menü können Sie die Liste der Anwendungen als csv- oder txt-Datei exportieren.

Detaillierte Informationen über die Programmkontrolle finden Sie in der Hilfe für Kaspersky Endpoint Security für Linux und in der Hilfe für Kaspersky Endpoint Security für Windows.

Über Anwendungen von Drittanbietern

Kaspersky Security Center Linux kann Ihnen dabei helfen, auf Client-Geräten installierte Drittanbieter-Programme zu aktualisieren und die Schwachstellen in Drittanbieter-Programmen zu beheben. Kaspersky Security Center Linux kann Drittanbieter-Programme nur von der aktuell installierten Version auf die neueste Version aktualisieren.

Die Liste mit Drittanbieter-Programmen kann geändert werden und wird dynamisch aktualisiert. Sie können überprüfen, ob Sie Drittanbieter-Programme (die auf Benutzergeräten installiert sind) mit Kaspersky Security Center Linux aktualisieren können, indem Sie die Liste der verfügbaren Updates in der Kaspersky Security Center Web Console anzeigen.

Das im Folgenden beschriebene Verfahren dient ausschließlich dazu, die Liste der Drittanbieter-Programme anzuzeigen, die über Kaspersky Security Center Linux aktualisiert werden können. Das Ausführen der Schritte ruft die erforderlichen Informationen ab, ohne eine Aufgabe zu starten.

So zeigen Sie Liste der Drittanbieter-Programme an, die Sie über Kaspersky Security Center Linux aktualisieren können:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.
3. Geben Sie im Schritt **Einstellungen der neue Aufgabe** des Assistenten die folgenden Einstellungen an:

   a. Wählen Sie in der Dropdown-Liste **Anwendung** die Option **Kaspersky Security Center Linux** aus.

   b. Wählen Sie in dem Feld **Aufgabentyp** die Option **Erforderliche Updates installieren und Schwachstellen schließen** aus.
4. Wählen Sie im Schritt **Gültigkeitsbereich der Aufgabe** die Option **Verwaltete Geräte**.
5. Klicken Sie im Schritt **Regeln für die Installation von Updates festlegen** des Assistenten auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
6. Wählen Sie im Schritt **Regeltyp auswählen** des Assistenten die Option **Regel für Updates von Drittherstellern** aus.
7. Wählen Sie im Schritt **Allgemeine Kriterien** des Assistenten die Option **Alle Updates installieren (ausgenommen abgelehnte)** und klicken Sie anschließend auf **Weiter**.

Die Liste der Drittanbieter-Programme wird angezeigt.

Installieren von Software-Updates von Drittanbietern

Mit Kaspersky Security Center Linux können Sie Updates für Drittanbieter-Programme, die auf den verwalteten Geräten installiert sind, verwalten und in diesen Programmen durch die Installation der erforderlichen Updates Schwachstellen beheben.

Kaspersky Security Center Linux sucht mithilfe der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* nach Updates. Nach Abschluss dieser Aufgabe erhält der Administrationsserver eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die auf den Geräten installierten Drittanbieter-Programme, die Sie in den Eigenschaften der Aufgabe angegeben haben. Nachdem Sie die Informationen über die verfügbaren Updates überprüft haben, können Sie die Updates auf Ihren Geräten installieren.

Kaspersky Security Center Linux aktualisiert einige Programme, indem die vorherige Programmversion entfernt und die neue Version installiert wird.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, das Drittanbieter-Programm zu schließen, wenn es gerade geöffnet ist.

Aus Sicherheitsgründen werden alle Updates für Drittanbieter-Programme, die Sie mittels der Funktion "Schwachstellen- und Patch-Management" installieren, automatisch von den Kaspersky-Technologien auf Schadsoftware untersucht. Die Technologien werden zur automatischen Untersuchung von Dateien verwendet und umfassen die Virensuche, die statische und die dynamische Analyse, die Verhaltensanalyse in der Sandbox-Umgebung sowie Machine-Learning-Methoden.

Kaspersky-Experten führen keine manuelle Analyse von Updates für Drittanbieter-Programme durch, die mit der Funktion "Schwachstellen- und Patch-Management" installiert werden können. Darüber hinaus suchen Kaspersky-Experten in derartigen Updates weder nach Schwachstellen (bekannt und unbekannt) oder nicht dokumentierten Funktionen, noch führen sie an ihnen zusätzliche Analysen durch, die über die oben genannten hinausgehen.

Wenn die Metadaten von Updates für Drittanbieter-Programme in die Datenverwaltung heruntergeladen wurden, können Sie die Updates mithilfe der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* auf den Client-Geräten installieren.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* kann nur erstellt werden, wenn Sie eine Lizenz für das Schwachstellen- und Patch-Management besitzen.

Nach Abschluss dieser Aufgabe wurden die Updates automatisch auf den verwalteten Geräten installiert. Wenn die Metadaten der neuen Updates in die Datenverwaltung des Administrationsservers heruntergeladen wurden, prüft Kaspersky Security Center Linux, ob die Updates den Kriterien der Update-Regeln entsprechen. Alle neuen Updates, welche die Kriterien erfüllen, werden beim nächsten Aufgabenstart automatisch heruntergeladen und installiert.

Szenario: Aktualisieren von Software von Drittanbietern

Dieser Abschnitt enthält ein Szenario für das Update von Drittanbieter-Programmen, die auf Client-Geräten installiert sind. Als Drittanbieter-Programme gelten Anwendungen von anderen Softwareherstellern.

Erforderliche Voraussetzungen

Der Administrationsserver muss mit dem Internet verbunden sein, um Updates für Drittanbieter-Programme installieren zu können.

Schritte

Das Update von Drittanbieter-Programmen umfasst mehrere Schritte:

1. **Suche nach erforderlichen Updates**

   Führen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* aus, um die für die verwalteten Geräte erforderlichen Updates für Drittanbieter-Programme zu suchen. Nach Abschluss dieser Aufgabe erhält Kaspersky Security Center Linux eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die auf den Geräten installierten Drittanbieter-Programme, die Sie in den Aufgabeneigenschaften angegeben haben.

   Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird automatisch vom Schnellstartassistent für den Administrationsserver erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*, oder führen Sie den Schnellstartassistenten jetzt aus.

   > Sie können die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* nur für Windows-Geräte erstellen. Sie können diese Aufgabe nicht für Geräte mit anderen Betriebssystemen erstellen.

2. **Liste der gefundenen Updates anzeigen**

   Sehen Sie sich die Informationen zu verfügbaren Updates für Drittanbieter-Programme an und entscheiden Sie, welche Updates Sie installieren möchten. Um genaue Informationen über alle Updates anzuzeigen, klicken Sie in der Liste auf den Namen des Updates. Für jedes Update in der Liste können Sie auch eine Statistik zur Update-Installation auf Client-Geräten anzeigen.

3. **Installation von Updates konfigurieren**

   Wenn Kaspersky Security Center Linux die Liste der Updates für Drittanbieter-Programme erhalten hat, können Sie diese auf den Client-Geräten installieren, indem Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellen.

   > Sie können die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* nur für Windows-Geräte erstellen. Sie können diese Aufgabe nicht für Geräte mit anderen Betriebssystemen erstellen.

   Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* dient dazu, Updates für Microsoft-Programme zu installieren, einschließlich der Updates, die vom Windows-Update-Dienst angeboten werden, sowie Updates für die Software anderer Hersteller. Beachten Sie, dass die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* nur erstellt werden kann, wenn Sie eine Lizenz für das Schwachstellen- und Patch-Management besitzen.

   Um bestimmte Programm-Updates installieren zu können, müssen Sie den Endbenutzer-Lizenzvertrag (EULA) akzeptieren. Wenn Sie die EULA ablehnen, wird das Programm-Update nicht installiert.

   Sie können eine Aufgabe zur Update-Installation nach Zeitplan starten. Stellen Sie im Aufgabenzeitplan sicher, dass die Aufgabe zur Update-Installation erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen wurde.

4. **Aufgaben planen**

Um sicherzustellen, dass die Update-Liste immer auf dem neuesten Stand ist, planen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* so, dass sie regelmäßig automatisch ausgeführt wird. Standardmäßig ist für die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* der manuelle Start eingestellt.

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt haben, können Sie festlegen, dass sie mit der gleichen Häufigkeit ausgeführt wird wie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* oder seltener.

Stellen Sie beim Planen der Aufgaben sicher, dass die Aufgabe zum Installieren der Updates erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen ist.

5. **Updates für Drittanbieter-Programme genehmigen und ablehnen (optional)**

   Falls Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt haben, können Sie im Fenster mit den Aufgabeneigenschaften Regeln für die Update-Installation festlegen.

   Sie können für jede Regel die zu installierenden Updates abhängig vom Update-Status definieren: *Nicht definiert*, *Genehmigt* oder *Abgelehnt*. Sie können beispielsweise eine spezielle Aufgabe für Server erstellen und für diese Aufgabe festlegen, dass nur Updates mit dem Status *Genehmigt* installiert werden dürfen. Anschließend legen Sie für die Updates, die Sie installieren möchten, manuell den Status *Genehmigt* fest. In diesem Fall werden Updates, die den Status *Nicht definiert* oder *Abgelehnt* besitzen, nicht auf den in der Aufgabe angegebenen Servern installiert.

   Bei einer geringen Anzahl von Updates ist das Verwenden des Status *Genehmigt* für die Verwaltung der Update-Installation effizient. Für die Verwaltung vieler Updates können Sie die Regeln verwenden, die Sie in der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* konfigurieren können. Es wird empfohlen, den Status *Genehmigt* nur für jene Updates festzulegen, die den durch Regeln angegebenen Kriterien nicht entsprechen. Wenn Sie eine hohe Anzahl von Updates manuell genehmigen, sinkt die Leistung des Administrationsservers. Dadurch kann der Administrationsserver überlastet werden.

   Standardmäßig besitzen heruntergeladene Programm-Updates den Status *Nicht definiert*. Sie können den Status in der Liste **Software-Updates** auf *Genehmigt* oder *Abgelehnt* ändern (**Vorgänge** → **Patch-Management** → **Software-Updates**).

   Weitere Informationen finden Sie in den Anleitungen zum Genehmigen und Ablehnen von Updates für Drittanbieter-Programme.

6. **Aufgabe zur Update-Installation ausführen**

   Starten der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen*. Wenn Sie diese Aufgabe ausführen, werden die Updates heruntergeladen und auf den verwalteten Geräten installiert. Stellen Sie nach Abschluss der Aufgabe sicher, dass die Aufgabe in der Liste den Status *Erfolgreich beendet* hat.

7. **Bericht über die Ergebnisse der Update-Installation erstellen (optional)**

   Um eine detaillierte Statistik über die Update-Installation anzuzeigen, erstellen Sie den Bericht über die Installationsergebnisse der Updates von Drittanbieterprogrammen.

Ergebnisse

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt und angepasst haben, werden die Updates automatisch auf den verwalteten Geräten installiert. Wenn neue Updates in die Datenverwaltung des Administrationsservers heruntergeladen werden, prüft Kaspersky Security Center Linux, ob die Updates den Kriterien aus den Update-Regeln entsprechen. Alle neuen Updates, welche die Kriterien erfüllen, werden beim nächsten Aufgabenstart automatisch installiert.

Installationsoptionen der Updates für Drittanbieter-Programme

Sie können Updates für Drittanbieter-Programme und Updates aus Windows-Update auf verwalteten Geräten installieren, indem Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellen und ausführen. Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* kann nur erstellt werden, wenn Sie eine Lizenz für das Schwachstellen- und Patch-Management besitzen. Mit dieser Aufgabe können Sie Updates für Drittanbieter-Programme installieren.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, das Drittanbieter-Programm zu schließen, wenn es gerade geöffnet ist.

Optional können Sie eine Aufgabe erstellen, um die erforderlichen Updates auf folgende Weise zu installieren:

- Indem Sie die Update-Liste öffnen und anschließend angeben, welche Updates installiert werden sollen.

  Dadurch wird eine neue Aufgabe zum Installieren der ausgewählten Updates erstellt. Optional können Sie die ausgewählten Updates zu einer vorhandenen Aufgabe hinzufügen.

- Indem Sie den Assistenten für die Installation von Updates ausführen.

  Der Assistent für die Installation von Updates ist nur im Rahmen der Lizenz für Schwachstellen- und Patch-Management verfügbar.

  Der Assistent vereinfacht die Erstellung und Konfiguration einer Aufgabe zur Update-Installation und hilft dabei, redundante Aufgaben zu vermeiden, die dieselben zu installierenden Updates enthalten.

Updates für Drittanbieter-Programme mithilfe der Update-Liste installieren

So installieren Sie Updates für Drittanbieter-Programme mithilfe der Update-Liste:

1. Öffnen Sie die Update-Liste über einen der folgenden Pfade:

   - **Software-Verwaltung** → **Patch-Management** → **Software-Updates**.
   - **Asset-Verwaltung** → **Assets (Geräte)** → <Gerätename> → **Erweitert** → **Verfügbare Updates**.
   - **Software-Verwaltung** → **Drittanbieteranwendungen** → **Programm-Registry** → <Name der Anwendung> → **Verfügbare Updates**.

   Eine Liste der verfügbaren Updates wird angezeigt.

2. Aktivieren Sie die Kontrollkästchen neben den Updates, die Sie installieren möchten.

3. Klicken Sie auf **Updates installieren**. Wenn diese Schaltfläche nicht sichtbar ist, klicken Sie auf die Schaltfläche mit den drei Punkten und wählen Sie anschließend in der Dropdown-Liste die Option **Updates installieren** aus.

   Zum Installieren bestimmter Programm-Updates müssen Sie den Endbenutzer-Lizenzvertrag (EULA) akzeptieren. Wenn Sie die EULA ablehnen, wird das Programm-Update nicht installiert.

4. Wählen Sie eine der folgenden Varianten aus:

   - **Neue Aufgabe**

     Der Assistent für das Erstellen einer Aufgabe wird gestartet. Wenn Sie über die Lizenz für Schwachstellen- und Patch-Management verfügen, ist die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* vorausgewählt. Folgen Sie den Schritten des Assistenten, um die Erstellung der Aufgabe abzuschließen.

   - **Update installieren (Regel zur angegebenen Aufgabe hinzufügen)**

     Wählen Sie eine Aufgabe, der Sie die ausgewählten Updates hinzufügen möchten. Wenn Sie über die Lizenz für Schwachstellen- und Patch-Management Lizenz für Schwachstellen- und Patch-Management verfügen, wählen Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* aus. Eine neue Regel für die Installation der ausgewählten Updates wird der ausgewählten Aufgabe automatisch hinzugefügt. Die ausgewählten Updates werden den Aufgabeneigenschaften hinzugefügt.

     Das Fenster mit den Aufgabeneigenschaften wird geöffnet. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

   Wenn Sie sich entschieden haben, eine neue Aufgabe zu erstellen, so wird diese neue Aufgabe erstellt und in der Aufgabenliste unter **Aufgaben** angezeigt. Wenn Sie sich entschieden haben, die Aufgaben zu einer vorhandenen Aufgabe hinzuzufügen, werden die Updates in den Aufgabeneigenschaften gespeichert.

Um Updates für Drittanbieter-Programme zu installieren, müssen Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* starten. Sie können diese Aufgabe starten, indem Sie in der Aufgabenliste auf **Starten** klicken oder in den Eigenschaften der zu startenden Aufgabe einen Zeitplan festlegen. Stellen Sie im Aufgabenzeitplan sicher, dass die Aufgabe zur Update-Installation erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen wurde.

Installieren von Updates für Drittanbieter-Programme mithilfe des Assistenten für die Installation von Updates

Der Assistent für die Installation von Updates ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

So erstellen Sie eine Aufgabe zur Installation der Updates für Drittanbieter-Programme mithilfe des Assistenten für die Installation von Updates:

1. Gehen Sie im Hauptmenü zu **Software-Verwaltung** → **Patch-Management** → **Software-Updates**.

   Eine Liste verfügbarer Updates wird geöffnet.

2. Aktivieren Sie das Kontrollkästchen neben dem Update, das Sie installieren möchten.

3. Klicken Sie auf **Assistent zur Installation von Updates starten**.

   Der Assistent für die Installation von Updates wird gestartet. Die Seite **Wählen Sie die Aufgabe zur Installation von Updates aus** enthält die Liste aller vorhandenen Aufgaben der folgenden Arten an:

   - *Erforderliche Updates installieren und Schwachstellen schließen*
   - *Schwachstellen schließen*

4. Wenn der Assistent nur die Aufgaben anzeigen soll, mit denen das von Ihnen ausgewählte Update installiert werden kann, aktivieren Sie die Option **Nur Aufgaben anzeigen, die das Update installieren**.

5. Wählen Sie aus, wie Sie vorgehen möchten:

- Um eine vorhandene Aufgabe zu starten, aktivieren Sie das Kontrollkästchen neben der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* und klicken Sie anschließend auf **Starten**.

  Die Aufgabe wird im Hintergrundmodus durchgeführt. Es sind keine weiteren Aktionen erforderlich.

- So fügen Sie einer vorhandenen Aufgabe eine neue Regel hinzu:

  a. Aktivieren Sie das Kontrollkästchen neben dem Aufgabennamen und klicken Sie auf **Regel hinzufügen**.

  > Die Schaltfläche **Regel hinzufügen** ist deaktiviert, wenn Sie mehr als eine Aufgabe auswählen.

  Für die Aufgabe *Schwachstellen schließen* können Sie keine Regel hinzufügen. Wenn Sie eine Aufgabe des Typs *Schwachstellen schließen* auswählen, wird die folgende Meldung angezeigt: "*Verwenden Sie die Aufgabe 'Erforderliche Updates installieren und Schwachstellen schließen', um Updates zu installieren.*"

  b. Konfigurieren Sie im Schritt **Regel zur Installation des Updates erstellen** des Assistenten die neue Regel:

  - **Regel für die Installation von Updates dieser Ereigniskategorie**

    Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

    Wenn diese Option aktiviert ist, beheben die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als die Signifikanz des ausgewählten Updates (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht behoben.

    Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

    Diese Option ist standardmäßig deaktiviert.

    Diese Regel wird nicht angezeigt, wenn das ausgewählte Update die Ereigniskategorie *Unbekannt* hat.

  - **Regel für die Installation von Updates dieser Ereigniskategorie nach MSRC**

    Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie sich entschließen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

    Wenn diese Option aktiviert ist (nur für Windows Update verfügbar), schließen die Updates nur jene Schwachstellen, für welche die vom Microsoft Security Response Center (MSRC) festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Niedrig**, **Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

    Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

    Diese Option ist standardmäßig deaktiviert.

    Diese Regel wird nur für Updates für Software von Microsoft angezeigt. Sie wird nicht angezeigt, wenn das ausgewählte Update die Ereigniskategorie *Unbekannt* hat.

  - **Regel für die Installation von Updates dieses Herstellers**

Diese Option ist nur für Updates von Drittanbieter-Programmen verfügbar. Kaspersky Security Center Linux installiert nur die Updates, die sich auf Programme beziehen, die vom selben Hersteller wie das ausgewählte Update erstellt wurden. Abgelehnte Updates und Updates für Programme anderer Hersteller werden nicht installiert.

Diese Option ist standardmäßig deaktiviert.

Diese Regel wird nur für Updates für Drittanbieter-Programme angezeigt.

- **Regel für die Installation von Updates vom Typ**
- **Regel für die Installation von Updates der ausgewählten Anwendung**

  Diese Regel wird nur für Software-Updates von Drittanbietern angezeigt.

- **Regel für die Installation des ausgewählten Updates**
- **Ausgewählte Updates bestätigen**

  Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

  Diese Option ist standardmäßig deaktiviert.

- **Alle vorherigen Anwendungs-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

  Lassen Sie diese Option aktiviert, wenn Sie mit der Installation von Programm-Zwischenversionen einverstanden sind, falls dies für die Installation der ausgewählten Updates erforderlich ist.

  Wenn diese Option deaktiviert ist, werden nur die ausgewählten Versionen von Programmen installiert. Deaktivieren Sie diese Option, wenn Sie Programme auf direkte Weise aktualisieren möchten, ohne zu versuchen, Nachfolgeversionen inkrementell zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

  Beispiel: Version 3 eines Programms ist auf einem Gerät installiert, und Sie möchten das Programm auf Version 5 aktualisieren. Version 5 dieses Programms kann aber nur über Version 4 installiert werden. Wenn diese Option aktiviert ist, installiert die Software zuerst Version 4 und installiert dann Version 5. Wenn diese Option deaktiviert ist, kann die Software das Programm nicht aktualisieren.

  Diese Option ist standardmäßig aktiviert.

c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Das Fenster mit den Aufgabeneigenschaften wird geöffnet. Die neue Regel wurde den Aufgabeneigenschaften hinzugefügt. Sie können die Regel oder andere Aufgabeneigenschaften anzeigen und anpassen. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

- So erstellen Sie eine Aufgabe:

  a. Klicken Sie auf **Neue Aufgabe**.

  b. Konfigurieren Sie im Schritt **Regel zur Installation des Updates erstellen** des Assistenten die neue Regel:

  - **Regel für die Installation von Updates dieser Ereigniskategorie**

    Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

Wenn diese Option aktiviert ist, beheben die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als die Signifikanz des ausgewählten Updates (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht behoben.

Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

Diese Option ist standardmäßig deaktiviert.

Diese Regel wird nicht angezeigt, wenn das ausgewählte Update die Ereigniskategorie *Unbekannt* hat.

- **Regel für die Installation von Updates dieser Ereigniskategorie nach MSRC**

  Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie sich entschließen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

  Wenn diese Option aktiviert ist (nur für Windows Update verfügbar), schließen die Updates nur jene Schwachstellen, für welche die vom Microsoft Security Response Center (MSRC) festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Niedrig**, **Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

  Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

  Diese Option ist standardmäßig deaktiviert.

  Diese Regel wird nur für Updates für Software von Microsoft angezeigt. Sie wird nicht angezeigt, wenn das ausgewählte Update die Ereigniskategorie *Unbekannt* hat.

- **Regel für die Installation von Updates dieses Herstellers**

  Diese Option ist nur für Updates von Drittanbieter-Programmen verfügbar. Kaspersky Security Center Linux installiert nur die Updates, die sich auf Programme beziehen, die vom selben Hersteller wie das ausgewählte Update erstellt wurden. Abgelehnte Updates und Updates für Programme anderer Hersteller werden nicht installiert.

  Diese Option ist standardmäßig deaktiviert.

  Diese Regel wird nur für Updates für Drittanbieter-Programme angezeigt.

- **Regel für die Installation von Updates vom Typ**

- **Regel für die Installation von Updates der ausgewählten Anwendung**

  Diese Regel wird nur für Software-Updates von Drittanbietern angezeigt.

- **Regel für die Installation des ausgewählten Updates**

- **Ausgewählte Updates bestätigen**

  Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

  Diese Option ist standardmäßig deaktiviert.

- **Alle vorherigen Anwendungs-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

Lassen Sie diese Option aktiviert, wenn Sie mit der Installation von Programm-Zwischenversionen einverstanden sind, falls dies für die Installation der ausgewählten Updates erforderlich ist.

Wenn diese Option deaktiviert ist, werden nur die ausgewählten Versionen von Programmen installiert. Deaktivieren Sie diese Option, wenn Sie Programme auf direkte Weise aktualisieren möchten, ohne zu versuchen, Nachfolgeversionen inkrementell zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

Beispiel: Version 3 eines Programms ist auf einem Gerät installiert, und Sie möchten das Programm auf Version 5 aktualisieren. Version 5 dieses Programms kann aber nur über Version 4 installiert werden. Wenn diese Option aktiviert ist, installiert die Software zuerst Version 4 und installiert dann Version 5. Wenn diese Option deaktiviert ist, kann die Software das Programm nicht aktualisieren.

Diese Option ist standardmäßig aktiviert.

c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Fahren Sie mit der Erstellung der Aufgabe im Assistenten für das Erstellen einer Aufgaben fort. Die neue Regel, die Sie im Assistenten für die Installation von Updates hinzugefügt haben, wird im Assistenten für das Erstellen einer Aufgaben angezeigt. Wenn Sie den Assistenten abgeschlossen haben, wird die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* zur Aufgabenliste hinzugefügt.

Einstellungen der Aufgabe zur Suche nach Schwachstellen und erforderlichen Updates

Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird automatisch erstellt, wenn der Schnellstartassistent ausgeführt wird. Wenn Sie den Assistenten nicht ausgeführt haben, können Sie die Aufgabe manuell erstellen.

Neben den allgemeinen Aufgabeneinstellungen können Sie die folgenden Einstellungen vornehmen, wenn Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* erstellen oder wenn Sie die Eigenschaften der erstellten Aufgabe später konfigurieren:

- **Nach Schwachstellen und Updates suchen, die von Microsoft gelistet werden**

  Wenn Kaspersky Security Center Linux nach Schwachstellen und Updates sucht, verwendet die Anwendung die Informationen über geeignete Microsoft-Updates aus der Quelle für momentan verfügbare Microsoft-Updates.

  Sie können diese Funktion deaktivieren, wenn Sie beispielsweise verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft-Updates und für Updates für Drittanbieter-Anwendungen haben.

  Diese Option ist standardmäßig aktiviert.

  Informationen über optionale Microsoft Windows-Updates werden nicht an den Administrationsserver übertragen.

- **Mit dem Update-Server verbinden, um Daten zu aktualisieren**

  Der Windows-Update-Agent auf einem verwalteten Gerät stellt eine Verbindung zur Quelle für Microsoft-Updates her. Die folgenden Server können als Quelle für Microsoft-Updates dienen:

  - Windows Server mit Microsoft Windows Server Update Services (WSUS), das in Ihrem Unternehmensnetzwerk bereitgestellt wurde
  - Microsoft-Update-Server

Wenn diese Option aktiviert ist, stellt der Windows-Update-Agent auf einem verwalteten Gerät eine Verbindung zur Quelle für Microsoft-Updates her, um die Informationen über geeignete Microsoft-Windows-Updates zu aktualisieren.

Wenn diese Option deaktiviert ist, verwendet der Windows-Update-Agent auf einem verwalteten Gerät die Informationen über geeignete Microsoft Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden.

Das Herstellen einer Verbindung zur Quelle für Microsoft-Updates kann ressourcenaufwendig sein. Sie können diese Option deaktivieren, wenn Sie in einer anderen Aufgabe oder in den Eigenschaften der Administrationsagenten-Richtlinie im Abschnitt **Software-Updates und Schwachstellen** eine regelmäßige Verbindung zu dieser Update-Quelle festgelegt haben. Wenn Sie diese Option nicht deaktivieren möchten, können Sie den Aufgabenzeitplan so anpassen, dass die Aufgabenstarts innerhalb von 360 Minuten zufällig verzögert werden, um eine Überlastung des Servers zu vermeiden.

Diese Option ist standardmäßig aktiviert.

Der Modus für den Update-Download beruht auf einer Kombination der folgenden Optionen, die in den Einstellungen der Administrationsagenten-Richtlinie festgelegt werden:

- Der Windows-Update-Agent auf einem verwalteten Gerät stellt nur unter den folgenden Bedingungen eine Verbindung zum Update-Server her, um Updates zu erhalten: Die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** in den Eigenschaften der Aufgabe zum *Suche nach Schwachstellen und erforderlichen Updates* ist aktiviert und die Option **Modus für die Suche nach Windows-Updates** steht in den Einstellungen der Administrationsagent-Richtlinie auf **Aktiv**.

- Wenn Sie den Administrationsagenten nicht benötigen, um während der Ausführung der Aufgabe *Untersuchung auf Schwachstellen* eine Verbindung zur Microsoft Windows-Update-Quelle herzustellen und Updates herunterzuladen, können Sie die Option **Modus für die Suche nach Windows-Updates** auf **Offline** setzen, wobei die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert bleiben muss. Auf diese Weise können Sie Ressourcen sparen und zuvor abgerufene Windows-Updates verwenden, um nach Schwachstellen zu suchen. Sie können den passiven Modus verwenden, wenn Sie das Abrufen von Microsoft Windows-Updates auf eine andere Art konfigurieren. Wenn das Abrufen von Microsoft Windows-Updates jedoch nicht auf eine andere Art konfiguriert ist, setzen Sie die Option **Modus für die Suche nach Windows-Updates** nicht auf **Offline**, da in diesem Fall keine Informationen über Updates abgerufen werden.

- Wenn die Option **Modus für die Suche nach Windows-Updates** auf **Deaktiviert** steht, fragt Kaspersky Security Center Linux keine Informationen über Updates ab. Der Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert) hat darauf keinen Einfluss darauf.

Wenn im Netzwerk Ihrer Organisation ein WSUS-Server (lokaler WSUS-Server) verwendet wird und Sie diesen zusammen mit dem Kaspersky Security Center Administrationsserver verwenden möchten, müssen Sie zunächst sicherstellen, dass der Kaspersky Security Center Administrationsserver nicht als WSUS-Server verwendet wird. Anschließend gehen Sie wie folgt vor:

1. Geben Sie auf Ihren verwalteten Windows-Geräten Ihren lokalen WSUS-Server für den Windows Update-Dienst an. Sie können dies entweder manuell in der Windows-Registry oder mithilfe einer Windows-Gruppenrichtlinie tun.

2. Legen Sie auf Ihrem lokalen WSUS-Server die erforderlichen Update-Klassifizierungen und die Anwendungen, an welche die Updates verteilt werden sollen, fest.

3. Synchronisieren Sie Ihren WSUS-Server mit dem Upstream-Server (das kann entweder ein Microsoft WSUS-Server oder ein anderer lokaler Upstream-WSUS-Server sein).

Nachdem die Aufgabe *Finden von Schwachstellen und erforderlichen Updates* auf dem Gerät ausgeführt wurde, verwendet der Administrationsagent den Windows Update-Dienst, um eine Anfrage für Windows-Updates zu initiieren, die auf dem Gerät anwendbar sind. Der Windows Update-Dienst bezieht die Adresse des externen WSUS-Servers aus der Registry und sucht auf diesem externen WSUS-Server direkt nach Updates. Anschließend leitet der Windows Update-Dienst diese Liste über den Administrationsagenten an den Administrationsserver weiter. Damit verfügt der Administrationsserver über eine aktuelle Update-Grundlage.

- **Nach Schwachstellen und Updates von Drittanbietern suchen, die von Kaspersky gelistet werden**

  Wenn diese Option aktiviert ist, sucht Kaspersky Security Center Linux in der Windows-Registrierung und den unter **Geben Sie Pfade zur erweiterten Suche von Anwendungen im Dateisystem an** festgelegten Ordnern nach Schwachstellen und erforderlichen Updates für Drittanbieter-Produkte (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft stammen). Die vollständige Liste der unterstützten Drittanbieter-Anwendungen wird von Kaspersky verwaltet.

  Wenn diese Option deaktiviert ist, sucht Kaspersky Security Center Linux nicht nach Schwachstellen und erforderlichen Updates für Drittanbieter-Anwendungen. Sie können diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft Windows-Updates und Updates für Drittanbieter-Anwendungen haben.

  Diese Option ist standardmäßig aktiviert.

- **Pfade für die erweiterte Suche nach Anwendungen im Dateisystem angeben**

  Die Ordner, in denen Kaspersky Security Center Linux nach Drittanbieter-Anwendungen sucht, in denen Schwachstellen behoben und Updates installiert werden müssen. Sie können Systemvariablen verwenden.

  Legen Sie die Ordner fest, in denen Programme installiert sind. Standardmäßig enthält die Liste die Systemordner, in denen die meisten Programme installiert sind.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, legt der Administrationsagent Protokolldateien auch dann an, wenn das Erstellen von Protokolldateien für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center Linux deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Remote-Diagnose-Tool zugegriffen werden. Dort können Sie die Dateien herunterladen oder löschen.

  Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Remote-Diagnose-Tool für Kaspersky Security Center Linux durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, falls die Informationen in von Ihnen gesendeten Dateien der erweiterten Diagnose nicht ausreichen, um das Problem zu beheben.

Tipps für den Aufgabenzeitplan

Stellen Sie bei der Planung der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* sicher, dass die beiden Optionen **Übersprungene Aufgaben starten** und **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** aktiviert sind.

Standardmäßig ist für die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* der manuelle Start eingestellt. Wenn zu diesem Zeitpunkt alle Geräte aufgrund der Regeln und Vorschriften des Unternehmens deaktiviert sind, wird die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* ausgeführt, nachdem die Geräte wieder eingeschaltet werden (also am Morgen des folgenden Tages). Ein solches Verhalten kann unerwünscht sein, da die Untersuchung auf Schwachstellen eine erhöhte Belastung des Prozessors und des Laufwerkssubsystems verursachen kann. Für einen optimalen Aufgabenzeitplan sollten die im Unternehmen geltenden Regeln und Vorschriften berücksichtigt werden.

Erstellen der Aufgabe "Suche nach Schwachstellen und erforderlichen Updates"

Über die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* erhält Kaspersky Security Center Linux eine Listen mit erkannten Schwachstellen und erforderlichen Updates für die Software von Drittanbietern, die auf den verwalteten Geräten installiert ist.

> Sie können die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* nur für Windows-Geräte erstellen. Sie können diese Aufgabe nicht für Geräte mit anderen Betriebssystemen erstellen.

Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird automatisch erstellt, wenn der Schnellstartassistent ausgeführt wird. Wenn Sie den Assistenten nicht ausgeführt haben, erstellen Sie die Aufgabe manuell.

So erstellen Sie die Aufgabe Suche nach Schwachstellen und erforderlichen Updates:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.
2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.
3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Suche nach Schwachstellen und erforderlichen Updates**.
4. Geben Sie den Namen für die Aufgabe an, die Sie anlegen. Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.
5. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.
6. Wählen Sie die Methoden für die Untersuchung auf Schwachstellen und die zu aktualisierenden Anwendungen aus:

   - **Nach Schwachstellen und Updates suchen, die von Microsoft gelistet werden**

     Wenn Kaspersky Security Center Linux nach Schwachstellen und Updates sucht, verwendet die Anwendung die Informationen über geeignete Microsoft-Updates aus der Quelle für momentan verfügbare Microsoft-Updates.

Sie können diese Funktion deaktivieren, wenn Sie beispielsweise verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft-Updates und für Updates für Drittanbieter-Anwendungen haben.

Diese Option ist standardmäßig aktiviert.

Informationen über optionale Microsoft Windows-Updates werden nicht an den Administrationsserver übertragen.

- **Mit dem Update-Server verbinden, um Daten zu aktualisieren**

  Der Windows-Update-Agent auf einem verwalteten Gerät stellt eine Verbindung zur Quelle für Microsoft-Updates her. Die folgenden Server können als Quelle für Microsoft-Updates dienen:

  - Windows Server mit Microsoft Windows Server Update Services (WSUS), das in Ihrem Unternehmensnetzwerk bereitgestellt wurde
  - Microsoft-Update-Server

  Wenn diese Option aktiviert ist, stellt der Windows-Update-Agent auf einem verwalteten Gerät eine Verbindung zur Quelle für Microsoft-Updates her, um die Informationen über geeignete Microsoft-Windows-Updates zu aktualisieren.

  Wenn diese Option deaktiviert ist, verwendet der Windows-Update-Agent auf einem verwalteten Gerät die Informationen über geeignete Microsoft Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden.

  Das Herstellen einer Verbindung zur Quelle für Microsoft-Updates kann ressourcenaufwendig sein. Sie können diese Option deaktivieren, wenn Sie in einer anderen Aufgabe oder in den Eigenschaften der Administrationsagenten-Richtlinie im Abschnitt **Software-Updates und Schwachstellen** eine regelmäßige Verbindung zu dieser Update-Quelle festgelegt haben. Wenn Sie diese Option nicht deaktivieren möchten, können Sie den Aufgabenzeitplan so anpassen, dass die Aufgabenstarts innerhalb von 360 Minuten zufällig verzögert werden, um eine Überlastung des Servers zu vermeiden.

  Diese Option ist standardmäßig aktiviert.

Der Modus für den Update-Download beruht auf einer Kombination der folgenden Optionen, die in den Einstellungen der Administrationsagenten-Richtlinie festgelegt werden:

- Der Windows-Update-Agent auf einem verwalteten Gerät stellt nur unter den folgenden Bedingungen eine Verbindung zum Update-Server her, um Updates zu erhalten: Die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** in den Eigenschaften der Aufgabe zum *Suche nach Schwachstellen und erforderlichen Updates* ist aktiviert und die Option **Modus für die Suche nach Windows-Updates** steht in den Einstellungen der Administrationsagent-Richtlinie auf **Aktiv**.

- Wenn Sie den Administrationsagenten nicht benötigen, um während der Ausführung der Aufgabe *Untersuchung auf Schwachstellen* eine Verbindung zur Microsoft Windows-Update-Quelle herzustellen und Updates herunterzuladen, können Sie die Option **Modus für die Suche nach Windows-Updates** auf **Offline** setzen, wobei die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert bleiben muss. Auf diese Weise können Sie Ressourcen sparen und zuvor abgerufene Windows-Updates verwenden, um nach Schwachstellen zu suchen. Sie können den passiven Modus verwenden, wenn Sie das Abrufen von Microsoft Windows-Updates auf eine andere Art konfigurieren. Wenn das Abrufen von Microsoft Windows-Updates jedoch nicht auf eine andere Art konfiguriert ist, setzen Sie die Option **Modus für die Suche nach Windows-Updates** nicht auf **Offline**, da in diesem Fall keine Informationen über Updates abgerufen werden.

- Wenn die Option **Modus für die Suche nach Windows-Updates** auf **Deaktiviert** steht, fragt Kaspersky Security Center Linux keine Informationen über Updates ab. Der Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert) hat darauf keinen Einfluss darauf.

Wenn im Netzwerk Ihrer Organisation ein WSUS-Server (lokaler WSUS-Server) verwendet wird und Sie diesen zusammen mit dem Kaspersky Security Center Administrationsserver verwenden möchten, müssen Sie zunächst sicherstellen, dass der Kaspersky Security Center Administrationsserver nicht als WSUS-Server verwendet wird. Anschließend gehen Sie wie folgt vor:

1. Geben Sie auf Ihren verwalteten Windows-Geräten Ihren lokalen WSUS-Server für den Windows Update-Dienst an. Sie können dies entweder manuell in der Windows-Registry oder mithilfe einer Windows-Gruppenrichtlinie tun.

2. Legen Sie auf Ihrem lokalen WSUS-Server die erforderlichen Update-Klassifizierungen und die Anwendungen, an welche die Updates verteilt werden sollen, fest.

3. Synchronisieren Sie Ihren WSUS-Server mit dem Upstream-Server (das kann entweder ein Microsoft WSUS-Server oder ein anderer lokaler Upstream-WSUS-Server sein).

Nachdem die Aufgabe *Finden von Schwachstellen und erforderlichen Updates* auf dem Gerät ausgeführt wurde, verwendet der Administrationsagent den Windows Update-Dienst, um eine Anfrage für Windows-Updates zu initiieren, die auf dem Gerät anwendbar sind. Der Windows Update-Dienst bezieht die Adresse des externen WSUS-Servers aus der Registry und sucht auf diesem externen WSUS-Server direkt nach Updates. Anschließend leitet der Windows Update-Dienst diese Liste über den Administrationsagenten an den Administrationsserver weiter. Damit verfügt der Administrationsserver über eine aktuelle Update-Grundlage.

- **Nach Schwachstellen und Updates von Drittanbietern suchen, die von Kaspersky gelistet werden**

  Wenn diese Option aktiviert ist, sucht Kaspersky Security Center Linux in der Windows-Registrierung und den unter **Geben Sie Pfade zur erweiterten Suche von Anwendungen im Dateisystem an** festgelegten Ordnern nach Schwachstellen und erforderlichen Updates für Drittanbieter-Produkte (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft stammen). Die vollständige Liste der unterstützten Drittanbieter-Anwendungen wird von Kaspersky verwaltet.

Wenn diese Option deaktiviert ist, sucht Kaspersky Security Center Linux nicht nach Schwachstellen und erforderlichen Updates für Drittanbieter-Anwendungen. Sie können diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft Windows-Updates und Updates für Drittanbieter-Anwendungen haben.

Diese Option ist standardmäßig aktiviert.

Sie können diese Optionen nach der Erstellung der Aufgabe auf der Registerkarte **Anwendungseinstellungen** im Eigenschaftenfenster der Aufgabe deaktivieren.

7. **Pfade für die erweiterte Suche nach Anwendungen im Dateisystem angeben**

   Die Ordner, in denen Kaspersky Security Center Linux nach Drittanbieter-Anwendungen sucht, in denen Schwachstellen behoben und Updates installiert werden müssen. Sie können Systemvariablen verwenden.

   Legen Sie die Ordner fest, in denen Programme installiert sind. Standardmäßig enthält die Liste die Systemordner, in denen die meisten Programme installiert sind.

   Sie können die angegebenen Pfade nach der Erstellung der Aufgabe auf der Registerkarte **Anwendungseinstellungen** im Eigenschaftenfenster der Aufgabe ändern.

8. Aktivieren Sie bei Bedarf die **Erweiterte Diagnose aktivieren**

   Wenn diese Funktion aktiviert ist, legt der Administrationsagent Protokolldateien auch dann an, wenn das Erstellen von Protokolldateien für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center Linux deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Remote-Diagnose-Tool zugegriffen werden. Dort können Sie die Dateien herunterladen oder löschen.

   Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Remote-Diagnose-Tool für Kaspersky Security Center Linux durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

   Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

   Diese Option ist standardmäßig deaktiviert.

   Sie können diese Option nach der Erstellung der Aufgabe auf der Registerkarte **Anwendungseinstellungen** im Eigenschaftenfenster der Aufgabe deaktivieren.

9. Geben Sie die **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** an

   Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, falls die Informationen in von Ihnen gesendeten Dateien der erweiterten Diagnose nicht ausreichen, um das Problem zu beheben.

   Wenn Sie im vorherigen Schritt die erweiterte Diagnose aktiviert haben, müssen Sie diesen Wert angeben. Sie können diesen Wert nach der Erstellung der Aufgabe auf der Registerkarte **Anwendungseinstellungen** im Eigenschaftenfenster der Aufgabe ändern.

10. Wenn Sie die Standardeinstellungen für Aufgaben ändern möchten, aktivieren Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** auf der Seite **Erstellung der Aufgabe abschließen**. Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später jederzeit ändern.

11. Klicken Sie auf die Schaltfläche **Fertigstellen**.

Der Assistent erstellt die Aufgabe. Wenn Sie die Option Nach **Nach Abschluss der Erstellung Aufgabendetails öffnen** haben, wird das Fenster mit Aufgabeneigenschaften automatisch geöffnet. In diesem Fenster können Sie die allgemeinen Aufgabeneinstellungen angeben und bei Bedarf die Einstellungen ändern, die bei der Aufgabenerstellung festgelegt wurden.

Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Aufgabenliste auf den Namen der erstellten Aufgabe klicken.

Die Aufgabe wird erstellt und konfiguriert. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie auf **Starten**.

Empfehlungen für den Aufgabenzeitplan

Stellen Sie bei der Planung der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* sicher, dass die beiden Optionen **Übersprungene Aufgaben starten** und **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** aktiviert sind.

Standardmäßig ist für die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* der manuelle Start eingestellt.

Sie können die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* auch so planen, dass sie zu einem bestimmten Zeitpunkt gestartet wird. Sie können beispielsweise als geplanten Start die Option **Alle n Stunden** in der Dropdown-Liste **Aufgabe starten** auf der Registerkarte **Zeitplan** des Fensters mit den Aufgabeneinstellungen auswählen. Beachten Sie dabei Folgendes: Wenn die Dienstvorschriften des Unternehmens zu dieser Zeit ein Deaktivieren der Geräte vorsehen, wird die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* ausgeführt, nachdem die Geräte wieder eingeschaltet wurden. Ein solches Verhalten kann unerwünscht sein, da die Untersuchung auf Schwachstellen eine erhöhte Belastung des Prozessors und des Laufwerkssubsystems verursachen kann. Es wird empfohlen, einen optimalen Zeitplan der Aufgabe basierend auf den im Unternehmen geltenden Dienstvorschriften zu konfigurieren.

Eine genaue Beschreibung der Einstellungen für den Start nach Zeitplan finden Sie in den allgemeinen Aufgabeneinstellungen.

Anzeigen von Informationen zu verfügbaren Updates von Drittanbieter-Programmen

Sie können die Liste der verfügbaren Updates für auf Client-Geräten installierte Drittanbieter-Programme, einschließlich für Software von Microsoft, anzeigen.

So zeigen Sie die Liste der Updates an, die für auf Client-Geräten installierte Drittanbieter-Anwendungen verfügbar sind:

Gehen Sie im Hauptmenü zu **Software-Verwaltung** → **Patch-Management** → **Software-Updates**.

Eine Liste der verfügbaren Updates wird angezeigt.

Sie können einen Filter angeben, um die Liste der Programm-Updates anzuzeigen. Klicken Sie in der Liste der Programm-Updates auf das **Filter**-Symbol ( ), um den Filter anzupassen. Sie können auch einen der voreingestellten Filter aus der Dropdown-Liste **Vordefinierte Filter** oberhalb der Liste mit Schwachstellen in Programmen auswählen.

So zeigen Sie die Eigenschaften eines Updates an:

1. Klicken Sie auf den Namen des gewünschten Programm-Updates.
2. Das Fenster mit den Update-Eigenschaften wird geöffnet. Es enthält die folgenden Registerkarten:

   - **Allgemein**

     Die Registerkarte enthält allgemeine Informationen über das ausgewählte Update:

     - Genehmigungsstatus des Updates (kann manuell durch Auswahl eines neuen Status in der Dropdown-Liste geändert werden)
     - Datum und Uhrzeit der Registrierung des Updates
     - Datum und Uhrzeit der Erstellung des Updates
     - Ereigniskategorie des Updates
     - Installationsvoraussetzungen, die für das Update gelten
     - Programmfamilie, zu der das Update gehört
     - Programm, zu dem das Update gehört
     - Revisionsnummer des Updates

   - **Attribute**

     Diese Registerkarte enthält eine Auswahl von Eigenschaften des Updates, die Sie verwenden können, um weitere Informationen über das Update zu erhalten. Die Auswahl unterscheidet sich je nachdem, ob es sich um ein Update von Microsoft oder von einem Drittanbieter handelt.

     Für ein Microsoft-Update enthält die Registerkarte die folgenden Informationen:

     - Ereigniskategorie des Updates, gemäß Microsoft Security Response Center (MSRC)
     - Link zu dem Artikel in der Microsoft Knowledge Base, in dem das Update beschrieben ist
     - Link zu dem Artikel in dem Microsoft-Sicherheitsbulletin, in dem das Update beschrieben ist
     - Update-Identifikator (ID)

     Für ein Drittanbieter-Update enthält die Registerkarte die folgenden Informationen:

     - Ob das Update ein Patch oder ein vollständiges Programmpaket ist
     - Lokalisierungssprache des Updates
     - Ob das Update automatisch oder manuell installiert wird
     - Ob das Update nach der Genehmigung widerrufen wurde
     - Download-Link für das Update

- **Geräte**

  Diese Registerkarte enthält eine Liste mit den Geräten, auf denen das ausgewählte Update installiert wurde.

- **Zu schließende Schwachstellen**

  Diese Registerkarte enthält eine Liste der Schwachstellen, die das ausgewählte Update schließen kann.

- **Überschneidungen von Updates**

  Diese Registerkarte enthält Überschneidungen von verschiedenen, für dasselbe Programm veröffentlichten Updates. Das heißt, ob das Update andere Updates ersetzen kann oder ob es selbst durch andere Updates ersetzt werden kann (nur für Microsoft-Updates verfügbar).

- **Aufgaben zur Installation des Updates**

  Diese Registerkarte enthält eine Liste der Aufgaben, deren Bereiche die Installation des ausgewählten Updates enthalten. Mit dieser Registerkarte können Sie auch eine neue Aufgabe zur Remote-Installation für das Update erstellen.

So zeigen Sie die Statistik für eine Update-Installation an:

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Programm-Update.

2. Klicken Sie auf **Statistik zum Status von Update-Installationen**.

Das Diagramm mit dem Update-Installationsstatus wird angezeigt. Wenn Sie auf einen Status klicken, wird eine Liste der Geräte mit dem ausgewählten Status geöffnet.

Sie können Informationen zu verfügbaren Updates für Drittanbieter-Programme, einschließlich für Software von Microsoft, die auf dem ausgewählten verwalteten Windows-Gerät installiert sind, anzeigen.

So zeigen Sie eine Liste der verfügbaren Updates für Drittanbieter-Programme an, die auf dem ausgewählten verwalteten Gerät installiert sind:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte)**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des Geräts, für das Sie die Updates für Drittanbieter-Programme anzeigen möchten.

   Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.

3. Wählen Sie im Eigenschaftenfenster des ausgewählten Geräts die Registerkarte **Erweitert** aus.

4. Wählen Sie im linken Fensterbereich den Abschnitt **Verfügbare Updates** aus. Wenn Sie nur installierte Updates anzeigen möchten, aktivieren Sie die Option **Installierte Updates anzeigen**.

Die Liste der verfügbaren Updates für Drittanbieter-Programme für das ausgewählte Gerät wird angezeigt.

Liste der verfügbaren Software-Updates in eine Datei exportieren

Sie können die Liste der Updates für Drittanbieter-Programme, einschließlich der Software von Microsoft, in eine csv- oder txt-Datei exportieren. Diese Dateien können Sie beispielsweise an Ihren Information Security Manager senden oder zu Statistikzwecken speichern.

So exportieren Sie die Liste der verfügbaren Updates für die Drittanbieter-Programme, die auf allen verwalteten Geräten installiert sind, in eine Textdatei:

1. Gehen Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Software-Updates**.

   Eine Liste der verfügbaren Updates wird angezeigt.

   Wenn Sie eine vollständige Liste der Programm-Updates exportieren möchten, werden nur die auf der aktuellen Seite sichtbaren Updates exportiert.

   Wenn Sie nur ausgewählte Updates exportieren möchten, aktivieren Sie in der Liste die Kontrollkästchen neben den gewünschten Updates.

2. Klicken Sie auf **In txt-Datei exportieren** oder **In csv-Datei exportieren**, je nachdem, welches Format Sie bevorzugen. Wenn keine dieser Schaltflächen sichtbar ist, klicken Sie auf die Schaltfläche mit den drei Punkten und wählen Sie anschießend in der Dropdown-Liste die gewünschte Option aus.

Die Datei mit der Liste an verfügbaren Updates für Drittanbieter-Programme, einschließlich der Software von Microsoft, wird auf Ihr aktuelles Gerät heruntergeladen.

So exportieren Sie die Liste der verfügbaren Updates für die Drittanbieter-Programme, die auf dem ausgewählten verwalteten Gerät installiert sind, in eine Textdatei:

1. Öffnen Sie die Liste der auf dem verwalteten Gerät verfügbaren Updates für Drittanbieter-Programme.

   Eine Liste der verfügbaren Updates wird angezeigt.

   Wenn Sie eine vollständige Liste der Programm-Updates exportieren möchten, werden nur die auf der aktuellen Seite sichtbaren Updates exportiert.

   Wenn Sie nur ausgewählte Updates exportieren möchten, aktivieren Sie in der Liste die Kontrollkästchen neben den gewünschten Updates.

   Wenn Sie nur installierte Updates exportieren möchten, aktivieren Sie das Kontrollkästchen **Installierte Updates anzeigen**.

2. Klicken Sie auf **In txt-Datei exportieren** oder **In csv-Datei exportieren**, je nachdem, welches Format Sie bevorzugen. Wenn keine dieser Schaltflächen sichtbar ist, klicken Sie auf die Schaltfläche mit den drei Punkten und wählen Sie anschießend in der Dropdown-Liste die gewünschte Option aus.

Die Datei mit der Liste an verfügbaren Updates für Drittanbieter-Programme (einschließlich der Software von Microsoft), die auf dem ausgewählten verwalteten Gerät installiert sind, wird auf Ihr aktuelles Gerät heruntergeladen.

Genehmigen und Ablehnen der Updates für Drittanbieter-Anwendungen

Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* anpassen, können Sie eine Regel erstellen, die einen bestimmten Status für zu installierende Updates voraussetzt. Eine Update-Regel kann beispielsweise die Installation der folgenden Updates zulassen:

- Nur genehmigte Updates
- Nur genehmigte und nicht definierte Updates
- Alle Updates unabhängig vom Update-Status

Sie können Updates, die installiert werden müssen, genehmigen und Updates, die nicht installiert werden dürfen, ablehnen.

Bei einer geringen Anzahl an Updates ist das Verwenden des Status *Genehmigt* für die Verwaltung der Update-Installation effizient. Für die Verwaltung vieler Updates können Sie die Regeln verwenden, die Sie in den Eigenschaften der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* konfigurieren können. Es wird empfohlen, den Status *Genehmigt* nur für die Updates zu setzen, die nicht den in den Regeln konfigurierten Kriterien entsprechen. Wenn Sie eine hohe Anzahl von Updates manuell genehmigen, sinkt die Leistung des Administrationsservers. Dadurch kann der Administrationsserver überlastet werden.

So genehmigen Sie ein oder mehrere Updates oder lehnen Updates ab:

1. Gehen Sie im Hauptmenü zu **Software-Verwaltung → Patch-Management → Software-Updates**.

   Die Liste mit den verfügbaren Updates wird geöffnet.

2. Wählen Sie die Updates aus, die Sie genehmigen oder ablehnen möchten.

3. Klicken Sie auf **Genehmigen**, um die ausgewählten Updates zu genehmigen, oder auf **Ablehnen**, um die ausgewählten Updates abzulehnen. Wenn keine dieser Schaltflächen sichtbar ist, klicken Sie auf die Schaltfläche mit den drei Punkten und wählen Sie anschließend in der Dropdown-Liste die gewünschte Option aus.

   Der Standardstatus eines Updates ist *Nicht definiert*.

Die ausgewählten Updates haben die Status, die Sie definiert haben.

Optional können Sie den Genehmigungsstatus in den Eigenschaften eines bestimmten Updates ändern.

So genehmigen Sie ein Update in dessen Eigenschaften oder lehnen ein Update ab:

1. Gehen Sie im Hauptmenü zu **Software-Verwaltung → Patch-Management → Software-Updates**.

   Die Liste mit den verfügbaren Updates wird geöffnet.

2. Klicken Sie auf den Namen des Updates, das Sie genehmigen oder ablehnen möchten.

   Das Fenster mit den Update-Eigenschaften wird geöffnet.

3. Legen Sie im Abschnitt **Allgemein** in der Dropdown-Liste **Status der Update-Genehmigung** einen Status für das Update fest. Sie können den Status *Genehmigt*, *Abgelehnt* oder *Nicht definiert* festlegen.

4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Das ausgewählte Update hat den Status, den Sie definiert haben.

Wenn Sie an Updates für Drittanbieter-Programme den Status *Abgelehnt* vergeben, werden diese Updates nicht auf jenen Geräten installiert, auf denen eine Installation vorgesehen war, aber noch nicht durchgeführt wurde. Auf den Geräten, auf denen die Updates bereits installiert sind, werden diese beibehalten. Bei Bedarf können Sie diese lokal manuell löschen.

Erstellen der Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen"

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* ist nur im Rahmen der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* wird verwendet, um Drittanbieter-Anwendungen, die auf verwalteten Geräten installiert sind, zu aktualisieren und Schwachstellen darin zu beheben. Mit dieser Aufgabe können Sie mehrere Updates installieren und mehrere Schwachstellen beheben. Entsprechende Regeln können Sie in den Aufgabeneinstellungen festlegen.

Es gibt folgende Möglichkeiten, um mithilfe der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* Updates zu installieren oder Schwachstellen zu beheben:

- Führen Sie den Assistenten für die Installation von Updates oder den Assistenten für das Schließen von Schwachstellen aus.
- Erstellen einer Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen*.
- Fügen Sie eine Regel für die Update-Installation zu einer bestehenden Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen* hinzu.

So erstellen Sie die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.

2. Klicken **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.

3. Wählen Sie in der Dropdown-Liste **Anwendung** die Option "Kaspersky Security Center" aus.

4. Wählen Sie in der Liste **Aufgabentyp** den Typ **Erforderliche Updates installieren und Schwachstellen schließen** aus.

   Wenn die Aufgabe nicht angezeigt wird, stellen Sie sicher, dass Ihr Benutzerkonto über die Berechtigungen **Lesen**, **Schreiben** und **Ausführen** für den Funktionsbereich **Systemverwaltung**: **Schwachstellen- und Patch-Management** verfügt. Ohne diese Zugriffsrechte können Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* nicht erstellen und konfigurieren.

5. Geben Sie im Feld **Aufgabenname** den Namen der neuen Aufgabe an.

   Der Aufgabenname darf höchstens 100 Zeichen lang sein und darf keine Sonderzeiten ("*<>?\:|) enthalten.

6. Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll.

7. Geben Sie beim Schritt **Regeln für die Installation von Updates festlegen** des Assistenten die Regeln für die Update-Installation an.

   Diese Regeln werden für die Installation von Updates auf Client-Geräten angewendet. Wenn keine Regeln festgelegt sind, wird die Aufgabe nicht ausgeführt. Informationen über Vorgänge mit Regeln finden Sie unter "Regeln zur Installation von Updates".

   Diese Regeln werden für die Installation von Updates auf Client-Geräten angewendet. Wenn Sie keine Regeln angeben, wird die Aufgabe nicht ausgeführt.

8. Geben Sie die folgenden Einstellungen an:

   - **Installation beim Neustart bzw. beim Herunterfahren des Geräts beginnen**

     Ist diese Option aktiviert, so werden Updates installiert, wenn das Gerät neu gestartet oder heruntergefahren wird. Andernfalls werden Updates nach einem Zeitplan installiert.

     Verwenden Sie diese Option, wenn die Installation von Updates die Geräteleistung beeinträchtigen könnte.

     Diese Option ist standardmäßig deaktiviert.

   - **Erforderliche allgemeine Systemkomponenten installieren**

     Wenn diese Option aktiviert ist, installiert die Anwendung vor der Installation eines Updates automatisch alle allgemeinen Systemkomponenten (erforderlichen Komponenten), die für die Installation des Updates erforderlich sind. Diese erforderlichen Komponenten können beispielsweise Updates des Betriebssystems sein.

     Wenn diese Option deaktiviert ist, müssen Sie die erforderlichen Komponenten möglicherweise manuell installieren.

     Diese Option ist standardmäßig deaktiviert.

   - **Installation einer neuen Anwendungsversion beim Update zulassen**

     Ist diese Option aktiviert, so werden Updates erlaubt, wenn sie zur Installation einer neuen Version einer Softwareanwendung führen.

     Wenn diese Option deaktiviert ist, wird die Software nicht aktualisiert. Sie können dann neue Versionen der Software manuell oder über eine andere Aufgabe installieren. Sie können diese Option beispielsweise verwenden, wenn die Infrastruktur Ihres Unternehmens nicht von einer neuen Softwareversion unterstützt wird oder wenn Sie ein Update in einer Testinfrastruktur überprüfen möchten.

     Diese Option ist standardmäßig aktiviert.

     > Das Update einer Anwendung kann zu Fehlern bei abhängigen Anwendungen führen, die auf Client-Geräten installiert sind.

   - **Updates auf das Gerät herunterladen, ohne sie zu installieren**

     Wenn diese Option aktiviert ist, lädt die Anwendung Updates auf das Gerät herunter, installiert sie jedoch nicht automatisch. Sie können die heruntergeladenen Updates dann manuell installieren.

     Microsoft-Updates werden in den Windows-Systemspeicher heruntergeladen. Updates für Drittanbieter-Anwendungen (Anwendungen, die von den Software-Herstellern Kaspersky oder Microsoft stammen) werden in den Ordner heruntergeladen, der im Feld **Updates herunterladen nach** angegeben ist.

Wenn diese Option deaktiviert ist, werden die Updates automatisch auf dem Gerät installiert.

Diese Option ist standardmäßig deaktiviert.

- **Updates herunterladen nach**

  Dieser Ordner wird verwendet, um Updates für Drittanbieter-Anwendungen (Anwendungen, die nicht von den Software-Herstellern Kaspersky oder Microsoft stammen) herunterzuladen.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, legt der Administrationsagent Protokolldateien auch dann an, wenn das Erstellen von Protokolldateien für den Administrationsagenten im Tool Remote-Diagnose für Kaspersky Security Center Linux deaktiviert ist. Die Ablaufverfolgung wird abwechselnd in zwei Dateien protokolliert; die Gesamtgröße beider Dateien wird durch den Wert **Maximale Größe der Dateien für die erweiterte Diagnose (MB)** bestimmt. Wenn beide Dateien voll sind, überschreibt der Administrationsagent alte Daten. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Remote-Diagnose-Tool zugegriffen werden. Dort können Sie die Dateien herunterladen oder löschen.

  Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Remote-Diagnose-Tool für Kaspersky Security Center Linux durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe müssen Sie die erweiterte Diagnose nicht aktivieren. Sie können diese Funktion später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen abrufen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB, und der Wert kann zwischen 1 MB und 2.048 MB liegen. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, falls die Informationen in von Ihnen gesendeten Dateien der erweiterten Diagnose nicht ausreichen, um das Problem zu beheben.

Gehen Sie zum nächsten Schritt des Assistenten.

9. Geben Sie die Einstellungen für den Neustart des Betriebssystems an:

- **Gerät nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

- **Gerät neu starten**

  Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

  Diese Option ist standardmäßig ausgewählt.

- **Aufforderung wiederholen alle (Min.)**

  Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

  Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten nach (Min.)**

  Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

  Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Erzwungenes Schließen von Anwendungen in gesperrten Sitzungen nach (Min.)**

  Programme werden zwangsweise geschlossen, wenn das Benutzergerät gesperrt wird (automatisch nach einer bestimmten Inaktivitätsdauer oder manuell).

  Wenn diese Option aktiviert ist, werden Programme auf einem gesperrten Gerät nach Ablauf der im Eingabefeld angegebenen Zeitspanne automatisch geschlossen.

  Wenn diese Option deaktiviert ist, werden Programme auf einem gesperrten Gerät nicht geschlossen.

  Diese Option ist standardmäßig deaktiviert.

10. Aktivieren Sie beim Schritt **Erstellung der Aufgabe abschließen** des Assistenten die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**, um die standardmäßigen Aufgabeneinstellungen zu ändern.

    Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später ändern.

11. Klicken Sie auf **Fertigstellen**.

    Der Assistent für das Erstellen einer Aufgabe erstellt die Aufgabe. Wenn Sie die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen** aktiviert haben, wird das Fenster mit den Aufgabeneigenschaften automatisch geöffnet. In diesem Fenster können Sie die allgemeinen Aufgabeneinstellungen angeben und bei Bedarf die Einstellungen ändern, die bei der Aufgabenerstellung festgelegt wurden.

    > Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Aufgabenliste auf den Namen der erstellten Aufgabe klicken.

    Die Aufgabe wurde erstellt und konfiguriert und wird in der Aufgabenliste angezeigt.

12. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf **Starten**.

Auf der Registerkarte **Zeitplan** im Eigenschaftenfenster der Aufgabe können Sie auch einen Zeitplan für den Aufgabenstart festlegen.

Eine genaue Beschreibung der Einstellungen für den Start nach Zeitplan finden Sie in den allgemeinen Aufgabeneinstellungen.

Nachdem die Aufgabe abgeschlossen ist, wurden die erforderlichen Updates installiert und die Schwachstellen behoben.

Wenn im Netzwerk Ihrer Organisation ein WSUS-Server (lokaler WSUS-Server) verwendet wird und Sie diesen zusammen mit dem Kaspersky Security Center Administrationsserver verwenden möchten, müssen Sie zunächst sicherstellen, dass der Kaspersky Security Center Administrationsserver nicht als WSUS-Server verwendet wird. Anschließend gehen Sie wie folgt vor:

a. Geben Sie auf Ihren verwalteten Windows-Geräten Ihren lokalen WSUS-Server für den Windows Update-Dienst an. Sie können dies entweder manuell in der Windows-Registry oder mithilfe einer Windows-Gruppenrichtlinie tun.

b. Legen Sie auf Ihrem lokalen WSUS-Server die erforderlichen Update-Klassifizierungen und die Anwendungen, an welche die Updates verteilt werden sollen, fest.

c. Synchronisieren Sie Ihren WSUS-Server mit dem Upstream-Server (das kann entweder ein Microsoft WSUS-Server oder ein anderer lokaler Upstream-WSUS-Server sein).

Nachdem die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* auf dem Gerät ausgeführt wurde, verwendet der Administrationsagent den Windows Update-Dienst, um Windows-Updates zu installieren. Der Windows Update-Dienst bezieht die Adresse des externen WSUS-Servers aus der Registry und lädt die Updates direkt von diesem externen WSUS-Server herunter.

Hinzufügen einer Regel für die Installation von Updates

Diese Funktion ist nur im Rahmen der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Beim Installieren von Programm-Updates oder beim Schließen von Schwachstellen in Programmen mittels der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* müssen Sie Regeln für die Update-Installation angeben. Diese Regeln bestimmen, welche Updates installiert und welche Schwachstellen geschlossen werden.

Die genauen Einstellungen hängen davon ab, ob Sie eine Regel für alle Updates, für Updates aus Windows-Update oder für Updates von Drittanbieter-Anwendungen (Anwendungen, die nicht von den Software-Herstellern Kaspersky oder Microsoft stammen) hinzufügen. Beim Hinzufügen einer Regel für Updates aus Windows-Update oder Updates von Drittanbieter-Anwendungen können Sie bestimme Programme und Programmversionen auswählen, für die Sie Updates installieren möchten. Beim Hinzufügen einer Regel für alle Updates können Sie bestimmte Updates, die Sie installieren möchten, und Schwachstellen, die Sie durch die Installation von Updates schließen möchten, auswählen.

Eine Regel für die Update-Installation können Sie auf folgende Arten hinzufügen:

- Durch Hinzufügen einer Regel beim Erstellen einer neuen Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen*.
- Durch Hinzufügen einer Regel auf der Registerkarte **Anwendungseinstellungen** in den Aufgabeneigenschaften einer bestehenden Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen*.
- Mittels des Assistenten für die Installation von Updates oder den Assistenten für das Schließen von Schwachstellen.

Regeln für alle Updates hinzufügen

So fügen Sie eine neue Regel für alle Updates hinzu:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

2. Wählen Sie im Schritt **Regeltyp auswählen** des Assistenten den Typ **Regel für alle Updates** aus.

3. Geben Sie im Schritt **Allgemeine Kriterien** des Assistenten die folgenden Einstellungen an:

   - **Auswahl der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.
     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht definiert* installiert.
     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

   Gehen Sie zum nächsten Schritt des Assistenten.

4. Wählen Sie die zu installierenden Updates aus:

   - **Alle relevanten Updates installieren**

     Installieren Sie alle Programm-Updates, von denen die im Assistenten unter dem Schritt **Allgemeine Kriterien** angeführten Kriterien erfüllt werden. Standardmäßig ausgewählt.

   - **Nur Updates aus der Liste installieren**

     Es werden nur Programm-Updates installiert, die Sie in der Liste manuell auswählen. Diese Liste enthält alle verfügbaren Programm-Updates.

     Sie können beispielsweise in den folgenden Fällen bestimmte Updates auswählen: um deren Installation in einer Testumgebung zu überprüfen, um nur kritische Programme zu aktualisieren oder um nur bestimmte Programme zu aktualisieren.

     - **Alle vorherigen Anwendungs-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

       Lassen Sie diese Option aktiviert, wenn Sie mit der Installation von Programm-Zwischenversionen einverstanden sind, falls dies für die Installation der ausgewählten Updates erforderlich ist.

       Wenn diese Option deaktiviert ist, werden nur die ausgewählten Versionen von Programmen installiert. Deaktivieren Sie diese Option, wenn Sie Programme auf direkte Weise aktualisieren möchten, ohne zu versuchen, Nachfolgeversionen inkrementell zu installieren. Wenn die Installation des ausgewählten Updates ohne Installation von vorherigen Versionen von Anwendungen nicht möglich ist, schlägt das Update der Anwendung fehl.

       Beispiel: Version 3 eines Programms ist auf einem Gerät installiert, und Sie möchten das Programm auf Version 5 aktualisieren. Version 5 dieses Programms kann aber nur über Version 4 installiert werden. Wenn diese Option aktiviert ist, installiert die Software zuerst Version 4 und installiert dann Version 5. Wenn diese Option deaktiviert ist, kann die Software das Programm nicht aktualisieren.

       Diese Option ist standardmäßig aktiviert.

   Gehen Sie zum nächsten Schritt des Assistenten.

5. Wählen Sie die Schwachstellen aus, die durch die Installation der ausgewählten Updates geschlossen werden:

   - **Alle Schwachstellen schließen, die den übrigen Kriterien entsprechen**

     Alle Schwachstellen schließen, welche die Kriterien im Schritt **Allgemeine Kriterien** des Assistenten erfüllen. Standardmäßig ausgewählt.

   - **Nur Schwachstellen aus der Liste schließen**

     Es werden nur Schwachstellen geschlossen, die Sie manuell aus der Liste auswählen. Diese Liste enthält alle gefundenen Schwachstellen.

     Sie können beispielsweise in den folgenden Fällen bestimmte Schwachstellen auswählen: um das Schließen in einer Testumgebung zu überprüfen, um Schwachstellen nur in kritischen Programmen zu schließen oder um Schwachstellen nur in bestimmten Programmen zu schließen.

   Gehen Sie zum nächsten Schritt des Assistenten.

6. Geben Sie den Namen für die hinzuzufügende Regel an. Sie können diesen Namen später auf der Registerkarte **Anwendungseinstellungen** in den Aufgabeneinstellungen der erstellten Aufgabe ändern.

Die neue Regel wurde erstellt und konfiguriert und wird in der Tabelle mit den Regeln des Assistent für das Erstellen einer Aufgabe angezeigt.

Regeln für Updates aus Windows-Update hinzufügen

So fügen Sie eine neue Regel für Updates aus Windows-Update hinzu:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

2. Wählen Sie **Regel für Windows-Updates** aus.

   Gehen Sie zum nächsten Schritt des Assistenten.

3. Geben Sie im Schritt **Allgemeine Kriterien** des Assistenten die folgenden Einstellungen an:

   - **Auswahl der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.
     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht definiert* installiert.
     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

   - **Schwachstellen schließen, deren MSRC-Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie sich entschließen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die vom Microsoft Security Response Center (MSRC) festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Niedrig**, **Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

4. Wählen Sie auf der Seite **Anwendungen** die Programme und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Wählen Sie auf der Seite **Update-Kategorien** die Kategorien der Updates aus, die installiert werden sollen. Diese Kategorien entsprechen den Kategorien im Microsoft-Update-Katalog. Standardmäßig sind alle Kategorien ausgewählt.

6. Geben Sie im Fenster **Name** den Namen der Regel an, die Sie hinzufügen. Sie können diesen Namen später im Abschnitt **Einstellungen** des Einstellungsfensters der erstellten Aufgabe ändern.

Nachdem dem Abschließen des Assistenten für neue Regeln wird die neue Regel hinzugefügt und in der Regelliste im Assistenten für das Erstellen einer Aufgaben oder in den Aufgabeneigenschaften angezeigt.

Regeln für Updates von Drittanbieter-Anwendungen hinzufügen

So fügen Sie eine neue Regel für Updates von Drittanbieter-Anwendungen hinzu:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Regel wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

2. Wählen Sie im Schritt **Regeltyp auswählen** des Assistenten den Typ **Regel für Updates von Drittherstellern** aus.

3. Geben Sie im Schritt **Allgemeine Kriterien** des Assistenten die folgenden Einstellungen an:

   - **Auswahl der zu installierenden Updates**

     Wählen Sie die Updates aus, die auf Client-Geräten installiert werden sollen:

     - **Nur bestätigte Updates installieren**. Damit werden nur bestätigte Updates installiert.

     - **Alle Updates installieren (ausgenommen abgelehnte)**. Damit werden Updates mit dem Genehmigungsstatus *Genehmigt* oder *Nicht definiert* installiert.

     - **Alle Updates installieren (einschließlich abgelehnte)**. Dies installiert alle Updates, unabhängig vom Genehmigungsstatus. Wählen Sie diese Option mit Bedacht. Sie können diese Option beispielsweise verwenden, wenn Sie die Installation einiger abgelehnter Updates in einer Testinfrastruktur überprüfen möchten.

   - **Schwachstellen schließen, deren Signifikanz gleich oder höher ist als**

     Manchmal können sich Software-Updates negativ auf die Benutzererfahrung mit der Software auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

     Wenn diese Option aktiviert ist, schließen die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Wert, der in der Liste ausgewählt ist (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht geschlossen.

     Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

     Diese Option ist standardmäßig deaktiviert.

   Gehen Sie zum nächsten Schritt des Assistenten.

4. Wählen Sie die Programme und Programmversionen aus, für die Sie Updates installieren möchten.

   Standardmäßig sind alle Programme ausgewählt.

Gehen Sie zum nächsten Schritt des Assistenten.

5. Geben Sie den Namen für die hinzuzufügende Regel an. Sie können diesen Namen später auf der Registerkarte **Anwendungseinstellungen** in den Aufgabeneinstellungen der erstellten Aufgabe ändern.

Die neue Regel wurde erstellt und konfiguriert und wird in der Tabelle mit den Regeln des Assistent für das Erstellen einer Aufgabe angezeigt.

Einstellungen der Aufgabe "Erforderliche Updates installieren und Schwachstellen schließen", die nach der Erstellung der Aufgabe angegeben wurden

Nachdem Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt haben, können Sie im Eigenschaftenfenster der Aufgabe auf der Registerkarte **Anwendungseinstellungen** die folgenden Einstellungen festlegen:

- Im Abschnitt **Testinstallation**:

  - **Nicht untersuchen**. Wählen Sie diese Option aus, wenn Sie keine Testinstallation von Updates ausführen möchten.

  - **Untersuchung auf den gewählten Geräten durchführen**. Wählen Sie diese Option aus, wenn Sie die Installation von Updates auf bestimmten Geräten testen möchten. Klicken Sie auf **Hinzufügen** und wählen Sie anschließend die Geräte aus, auf denen Sie eine Testinstallation von Updates ausführen möchten.

  - **Untersuchung auf den Geräten in der angegebenen Gruppe durchführen**. Wählen Sie diese Option aus, wenn Sie die Installation von Updates auf einer Gruppe von Geräten testen möchten. Geben Sie im Feld **Geben Sie eine Testgruppe an** eine Gruppe von Geräten an, auf denen eine Testinstallation ausgeführt werden soll.

  - **Untersuchung für den angegebenen Prozentsatz an Geräten durchführen**. Wählen Sie diese Option aus, wenn Sie die Installation von Updates auf einem prozentualen Anteil von Geräten testen möchten. Geben Sie im Feld **Prozentualer Anteil der Testgeräte an allen Zielgeräten** den Prozentanteil der Geräte an, auf denen Sie die Testinstallation von Updates ausführen möchten.

  Nachdem Sie eine beliebige Option ausgewählt haben (mit Ausnahme von **Nicht untersuchen**), geben Sie im Feld **Zeitspanne, um über das Fortsetzen der Installation zu entscheiden (Stunden)** die Anzahl an Stunden an, die nach der Testinstallation der Updates und vor dem Beginn der Update-Installation auf allen Geräten vergehen sollen.

- Im Abschnitt **Zu installierende Updates** können Sie die Liste der Updates anzeigen, die von der Aufgabe installiert werden. Es werden nur Updates angezeigt, die den übernommenen Aufgabeneinstellungen entsprechen.

Eine vollständige Beschreibung der Aufgabeneinstellungen finden Sie in den allgemeinen Aufgabeneinstellungen.

Automatisches Aktualisieren von Drittanbieter-Programmen

Einige Drittanbieter-Anwendungen können automatisch aktualisiert werden. Der Hersteller des jeweiligen Programms legt fest, ob das Programm die Auto-Update-Funktion unterstützt. Wenn eine auf einem verwalteten Gerät installierte Drittanbieter-Anwendung das automatische Update unterstützt, können Sie die Auto-Update-Option in den Anwendungseinstellungen konfigurieren. Nach einer Änderung der Auto-Update-Option wenden die Administrationsagenten die neuen Einstellungen auf alle verwalteten Geräte an, auf denen das Programm installiert ist.

Die Auto-Update-Option ist von den anderen Objekten und Einstellungen der Funktion für das Schwachstellen- und Patch-Management unabhängig. So ist diese Einstellung beispielsweise unabhängig vom Genehmigungsstatus eines Updates oder von den Aufgaben zur Update-Installation (z. B. *Erforderliche Updates installieren und Schwachstellen schließen* und *Schwachstellen schließen*).

So konfigurieren Sie die Auto-Update-Option für eine Drittanbieter-Anwendung:

1. Gehen Sie im Hauptmenü zu **Software-Verwaltung → Drittanbieteranwendungen → Programm-Registry**.
2. Klicken Sie auf den Namen des Programms, für das Sie die Auto-Update-Option ändern möchten.

   Um die Suche zu vereinfachen, können Sie Liste mithilfe der Spalten **Status des automatischen Updates** und **Automatisches Update verwalten** filtern.

   Das Fenster mit den Programmeinstellungen wird geöffnet.
3. Legen Sie im Abschnitt **Allgemein** einen Wert für die folgende Einstellung fest:

   Status des automatischen Updates.

   Wählen Sie eine der folgenden Varianten aus:

   - **Nicht definiert**

     Die Auto-Update-Funktion ist deaktiviert. Kaspersky Security Center Linux installiert Updates für Drittanbieter-Anwendungen unter Verwendung der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen* und *Schwachstellen schließen*.

   - **Zugelassen**

     Nachdem der Hersteller ein Update für das Programm veröffentlicht hat, wird es automatisch auf den verwalteten Geräten installiert. Es sind keine weiteren Aktionen erforderlich.

   - **Blockiert**

     Die Programm-Updates werden nicht automatisch installiert. Kaspersky Security Center Linux installiert Updates für Drittanbieter-Anwendungen unter Verwendung der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen* und *Schwachstellen schließen*.
4. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Die Auto-Update-Option wird auf das ausgewählte Programm angewendet.

Schwachstellen in Drittanbieter-Programmen schließen

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center Linux beschrieben, die sich auf das Schließen von Schwachstellen in den Programmen beziehen, die auf verwalteten Geräten installiert sind.

Über das Suchen und Schließen von Schwachstellen in Programmen

Kaspersky Security Center Linux erkennt und behebt Schwachstellen in Programmen auf verwalteten Geräten, auf denen Microsoft Windows-Betriebssysteme ausgeführt werden. Schwachstellen werden im Betriebssystem und in Drittanbieter-Programmen, einschließlich der Software von Microsoft, erkannt.

Die Update-Funktion (einschließlich der Bereitstellung von Updates für Antiviren-Signaturen und Codebases) sowie die KSN-Funktion sind möglicherweise in der Software in den USA nicht mehr verfügbar.

Software-Schwachstellen suchen

Kaspersky Security Center Linux verwendet Merkmale aus der Datenbank für bekannte Schwachstellen, um Software-Schwachstellen zu finden. Diese Datenbank wurde von den Kaspersky-Spezialisten erstellt und wird fortlaufend aktualisiert. Sie enthält Informationen zu Schwachstellen, z. B. eine Beschreibung, das Erkennungsdatum und die Signifikanz der Schwachstelle. Informationen über Software-Schwachstellen finden Sie auf der Kaspersky-Website.

Kaspersky Security Center Linux verwendet die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*, um Schwachstellen in Programmen zu finden.

Software-Schwachstellen schließen

Zum Beheben von Schwachstellen in Programmen verwendet Kaspersky Security Center Linux die Programm-Updates der Programmhersteller. Die Metadaten der Programm-Updates werden durch das Ausführen der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* in die Datenverwaltung des Administrationsservers heruntergeladen. Diese Aufgabe dient dazu, die Metadaten der Updates für Kaspersky-Anwendungen und Drittanbieter-Programme herunterzuladen. Diese Aufgabe wird vom Schnellstartassistenten des Kaspersky Security Centers Linux automatisch erstellt. Sie können die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* manuell erstellen.

Programm-Updates zur Behebung von Schwachstellen können in Form von vollständigen Programmpaketen oder Patches bereitgestellt werden. Programm-Updates, die Schwachstellen in Programmen beheben, werden als *Korrekturen* bezeichnet. *Empfohlene Korrekturen* sind solche, deren Installation von Kaspersky-Spezialisten empfohlen wird. *Individuelle Korrekturen* sind solche, die manuell für die Installation durch Benutzer ausgewählt werden. Um eine benutzerdefinierte Korrektur zu installieren, müssen Sie ein Installationspaket erstellen, das diese Korrektur enthält.

Wenn Sie für Kaspersky Security Center Linux eine Lizenz mit der Funktion "Schwachstellen- und Patch-Management" besitzen, können Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* verwenden. Diese Aufgabe behebt automatisch mehrere Schwachstellen, indem empfohlene Korrekturen installiert werden. Für diese Aufgabe können Sie bestimmte Regeln manuell konfigurieren, um mehrere Schwachstellen zu beheben.

Wenn Sie für Kaspersky Security Center Linux keine Lizenz mit der Funktion "Schwachstellen- und Patch-Management" besitzen, können Sie die Aufgabe *Schwachstellen schließen* verwenden. Mithilfe dieser Aufgabe können Sie Schwachstellen beheben, indem empfohlene Korrekturen für Software von Microsoft und individuelle Korrekturen für andere Drittanbieter-Programme installiert werden.

Aus Sicherheitsgründen werden alle Programm-Updates von Drittanbietern, die Sie mittels der Funktion "Schwachstellen- und Patch-Management" installieren, automatisch von den Kaspersky-Technologien auf Schadsoftware untersucht. Die Technologien werden zur automatischen Untersuchung von Dateien verwendet und umfassen die Virensuche, die statische und die dynamische Analyse, die Verhaltensanalyse in der Sandbox-Umgebung sowie Machine-Learning-Methoden.

Kaspersky-Experten führen keine manuelle Analyse von Updates für Drittanbieter-Programme durch, die mit der Funktion "Schwachstellen- und Patch-Management" installiert werden können. Darüber hinaus suchen Kaspersky-Experten in derartigen Updates weder nach Schwachstellen (bekannt und unbekannt) oder nicht dokumentierten Funktionen, noch führen sie an ihnen zusätzliche Analysen durch, die über die oben genannten hinausgehen.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie eine Drittanbieter-Anwendung aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einer Drittanbieter-Anwendung beheben. Beispielsweise kann der Benutzer aufgefordert werden, die Drittanbieter-Anwendung zu schließen, wenn es gerade geöffnet ist.

Zum Schließen bestimmter Software-Schwachstellen müssen Sie bei Aufforderung den Endbenutzer-Lizenzvertrag (EULA) für die Installation der Software akzeptieren. Wenn Sie die EULA ablehnen, kann die Schwachstelle nicht geschlossen werden.

Szenario: Finden und Schließen von Schwachstellen in Programmen von Drittanbietern

Dieser Abschnitt enthält ein Szenario zum Auffinden und Beheben von Schwachstellen auf verwalteten Windows-Geräten. Sie können Schwachstellen im Betriebssystem und in Programmen von Drittanbietern, einschließlich der Software von Microsoft, finden und schließen.

Erforderliche Vorrausetzungen

- Kaspersky Security Center Linux ist in Ihrem Unternehmen bereitgestellt.
- Sie haben in Ihrer Organisation verwaltete Geräte, auf denen Windows ausgeführt wird.
- Damit der Administrationsserver die folgenden Aufgaben ausführen kann, ist eine Internetverbindung erforderlich:
  - Erstellen einer Liste empfohlener Korrekturen für Schwachstellen in Software von Microsoft. Die Liste wird von Kaspersky-Spezialisten erstellt und regelmäßig aktualisiert.
  - Schwachstellen Drittanbieter-Programmen beheben, keine Software von Microsoft darstellen.

Schritte

Das Erkennen und Schließen von Schwachstellen in Programmen umfasst die folgenden Schritte:

1. **Scannen nach Schwachstellen in den auf den verwalteten Geräten installierten Programmen**

   Führen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* aus, um Schwachstellen in den auf den verwalteten Geräten installierten Programmen zu suchen. Nach Abschluss dieser Aufgabe erhält Kaspersky Security Center Linux eine Liste der erkannten Schwachstellen und der erforderlichen Updates für die die auf den Geräten installierten Drittanbieter-Programme, die Sie in den Eigenschaften der Aufgabe angegeben haben.

   Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird automatisch vom Schnellstartassistenten des Kaspersky Security Centers Linux erstellt. Wenn Sie den Assistenten nicht ausgeführt haben, starten Sie ihn jetzt oder erstellen Sie die Aufgabe manuell.

   > Sie können die Aufgabe *Finden von Schwachstellen und erforderlichen Updates* suchen nur für Windows-Geräte erstellen. Sie können diese Aufgabe nicht für Geräte mit anderen Betriebssystemen erstellen.

2. **Anzeigen der Liste der erkannten Schwachstellen in Programmen**

   Zeigen Sie die Liste **Schwachstellen in Programmen** an und entscheiden Sie, welche Schwachstellen in Programmen behoben werden müssen. Um detaillierte Informationen über alle Schwachstellen anzuzeigen, klicken Sie in der Liste auf den Namen der Schwachstelle. Für jede Schwachstelle in der Liste können Sie auch eine Statistik über die Schwachstelle auf den verwalteten Geräten anzeigen.

3. **Konfigurieren von Korrekturen für Schwachstellen**

   Wenn Schwachstellen in Programmen erkannt werden, können Sie diese auf den verwalteten Geräten schließen mithilfe der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen* oder *Schwachstellen schließen*.

   Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* wird verwendet, um Schwachstellen in Drittanbieter-Programmen (einschließlich der Software von Microsoft), die auf den verwalteten Geräten installiert ist, zu aktualisieren und zu beheben. Mit dieser Aufgabe können Sie mehrere Updates installieren und mehrere Schwachstellen nach bestimmten Regeln beheben. Beachten Sie, dass diese Aufgabe nur erstellt werden kann, wenn Sie eine Lizenz für die Funktion "Schwachstellen- und Patch-Management" haben. Um Schwachstellen in Programmen zu beheben, verwendet die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* die empfohlenen Programm-Updates.

   Die Aufgabe *Schwachstellen schließen* erfordert keine Lizenz-Option für die Funktion "Schwachstellen- und Patch-Management". Um die Aufgabe zu verwenden, müssen Sie manuell Individuelle Korrekturen angeben, um die Schwachstellen in Drittanbieter-Programmen zu beheben, die in den Aufgabeneinstellungen aufgeführt sind. Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für die Software von Microsoft und die individuellen Korrekturen für Drittanbieter-Programme.

   > Sie können die Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen* und *Schwachstellen schließen* nur für Windows-Geräte erstellen. Sie können diese Aufgaben nicht für Geräte mit anderen Betriebssystemen erstellen.

   Sie können entweder den Assistenten für das Schließen von Schwachstellen starten, der automatisch eine dieser Aufgaben erstellt, oder Sie können eine dieser Aufgaben manuell erstellen.

   Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt und angepasst haben, werden die Schwachstellen auf den verwalteten Geräten automatisch behoben. Beim Starten der erstellten Aufgabe wird die Liste der verfügbaren Programm-Updates mit den Regeln abgeglichen, die in den Aufgabeneinstellungen angegeben sind. Alle Programm-Updates, von denen die Kriterien der angegebenen Regeln erfüllt werden, werden in die Datenverwaltung des Administrationsservers heruntergeladen und installiert, um die Schwachstellen in Programmen zu beheben.

Wenn Sie die Aufgabe *Schwachstellen schließen* erstellt haben, werden nur Schwachstellen in der Software von Microsoft behoben.

4. **Aufgaben planen**

   Planen Sie die Ausführung der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* so, dass diese automatisch und in regelmäßigen Abständen gestartet wird. Auf diese Weise halten Sie die Liste der Schwachstellen auf dem neuesten Stand ist. Die empfohlene Häufigkeit beträgt einmal pro Woche.

   Wenn Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt haben, können Sie festlegen, dass sie mit der gleichen Häufigkeit ausgeführt wird wie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* oder seltener. Beachten Sie beim planen der Aufgabe *Schwachstellen schließen*, dass Sie vor jedem Start der Aufgabe entweder Patches für die Software von Microsoft auswählen oder individuelle Korrekturen für Drittanbieter-Programme angeben müssen.

   Stellen Sie beim Planen der Aufgaben sicher, dass die erstellte Aufgabe zum Beheben von Schwachstellen erst ausgeführt wird, nachdem die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* abgeschlossen ist.

5. **Ignorieren von Schwachstellen in Programmen (optional)**

   Das Ignorieren von bestimmten Schwachstelle in Programmen ist auf allen verwalteten Geräten oder nur auf dem ausgewählten Gerät möglich.

6. **Aufgabe zum Schließen von Schwachstellen ausführen**

   Starten Sie entweder die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* oder die Aufgabe *Schwachstellen schließen*. Stellen Sie nach Abschluss der Aufgabe sicher, dass sie in der Liste den Status *Erfolgreich beendet* besitzt.

7. **Bericht über die Ergebnisse des Schließens von Schwachstellen in Programmen erstellen (optional)**

   Generieren Sie den Bericht über Schwachstellen, um detaillierte Statistiken zu den behobenen Schwachstellen anzuzeigen. Dieser Bericht enthält Informationen über Schwachstellen in Programmen, die nicht behoben wurden. Er ermöglicht Ihnen für die Drittanbieter-Programme (einschließlich der Software von Microsoft), die in Ihrem Unternehmen verwendet werden, Schwachstellen zu identifizieren und zu beheben.

8. **Überprüfen der Konfiguration zum Finden und Schließen von Schwachstellen in Drittanbieter-Programmen**

   Stellen Sie sicher, dass folgende Aktionen ausgeführt wurden:

   - Abrufen und Überprüfen der Liste von Schwachstellen in Programmen auf verwalteten Geräten.
   - Ignorieren bestimmter Schwachstellen in Programmen, falls erwünscht.
   - Konfigurieren der Aufgabe zum Schließen von Schwachstellen.
   - Planen der Aufgaben zum Finden und Schließen von Schwachstellen in Programmen, sodass diese nacheinander gestartet werden.
   - Überprüfen, ob die Aufgabe zum Schließen von Schwachstellen in Programmen gestartet wurde.

Schwachstellen in Drittanbieter-Programmen schließen

Um Schwachstellen in Drittanbieter-Anwendungen zu finden, können Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* erstellen und ausführen und so eine Liste mit Software-Schwachstellen erhalten. Nachdem Sie die Liste mit den Software-Schwachstellen erstellt haben, können Sie die Schwachstellen auf den verwalteten Windows-Geräten beheben.

Das Schließen von Schwachstellen im Betriebssystem und in Drittanbieter-Anwendungen (einschließlich Software von Microsoft) ist mithilfe der Aufgaben Schwachstellen schließen oder Erforderliche Updates installieren und Schwachstellen schließen möglich.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, ein momentan geöffnetes Drittanbieter-Programm zu schließen.

Optional können Sie eine Aufgabe erstellen, um Schwachstellen in Programmen auf folgende Weise zu schließen:

- Öffnen Sie die Schwachstellenliste und geben Sie an, welche Schwachstellen geschlossen werden sollen.

  Dadurch wird eine neue Aufgabe zum Schließen von Software-Schwachstellen erstellt. Sie können die ausgewählten Schwachstellen auch zu einer vorhandenen Aufgabe hinzufügen.

- Führen Sie den Assistenten für das Schließen von Schwachstellen aus.

  Der Assistent für das Schließen von Schwachstellen ist nur im Rahmen der Lizenz für Schwachstellen- und Patch-Management verfügbar.

  Der Assistent vereinfacht die Erstellung und Konfiguration einer Aufgabe zum Schließen von Schwachstellen und hilft dabei, redundante Aufgaben zu vermeiden.

Software-Schwachstellen mithilfe der Schwachstellenliste schließen

So schließen Sie Schwachstellen in Programmen mithilfe der Schwachstellenliste:

1. Öffnen Sie die Schwachstellenliste, indem Sie einen der folgenden Schritte ausführen:

   - Gehen Sie im Hauptmenü zu **Software-Verwaltung** → **Patch-Management** → **Schwachstellen in Programmen**.
   - Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)** → <Gerätename> → **Erweitert** → **Schwachstellen in Programmen**.
   - Gehen Sie im Hauptmenü zu **Software-Verwaltung** → **Drittanbieteranwendungen** → **Programm-Registry** → <Anwendungsname> → **Schwachstellen**.

   Eine Tabelle mit der Liste von Schwachstellen in Drittanbieter-Anwendungen, die auf den verwalteten Geräten installiert sind, wird angezeigt.

2. Aktivieren Sie in der Schwachstellenliste die Kontrollkästchen neben den Schwachstellen, die Sie schließen möchten, und klicken Sie anschließend auf **Schwachstelle schließen**.

   Wenn das empfohlene Programm-Update zum Schließen einer ausgewählten Schwachstelle nicht vorhanden ist, erscheint eine Meldung.

   Zum Schließen bestimmter Software-Schwachstellen müssen Sie bei Aufforderung den Endbenutzer-Lizenzvertrag (EULA) für die Installation der Software akzeptieren. Wenn Sie die EULA ablehnen, kann die Schwachstelle nicht geschlossen werden.

3. Wählen Sie eine der folgenden Varianten aus:

   - **Neue Aufgabe**

     Der Assistent für das Erstellen einer Aufgabe wird gestartet. Wenn Sie über die Lizenz für Schwachstellen- und Patch-Management verfügen, ist die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen vorausgewählt. Wenn Sie diese Lizenz nicht haben, ist die Aufgabe Schwachstellen schließen vorausgewählt. Folgen Sie den Schritten des Assistenten, um die Erstellung der Aufgabe abzuschließen.

   - **Schwachstelle schließen (Regel zur angegebenen Aufgabe hinzufügen)**

     Wählen Sie eine Aufgabe, der Sie die ausgewählten Schwachstellen hinzufügen wollen. Wenn Sie über die Lizenz für Schwachstellen- und Patch-Management verfügen, wählen Sie die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen aus. Eine neue Regel zum Schließen der ausgewählten Schwachstellen wird der ausgewählten Aufgabe automatisch hinzugefügt. Wenn Sie diese Lizenz nicht haben, wählen Sie die Aufgabe Schwachstellen schließen aus. Die ausgewählten Updates werden den Aufgabeneigenschaften hinzugefügt.

     Das Fenster mit den Aufgabeneigenschaften wird geöffnet. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

   Wenn Sie sich entschieden haben, eine Aufgabe zu erstellen, so wird diese Aufgabe erstellt und in der Aufgabenliste unter **Aufgaben** angezeigt. Wenn Sie sich entschieden haben, die Schwachstellen zu einer vorhandenen Aufgabe hinzuzufügen, werden die Schwachstellen in den Aufgabeneigenschaften gespeichert.

Um Schwachstellen in Drittanbieter-Anwendungen zu schließen, starten Sie die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen oder die Aufgabe Schwachstellen schließen. Wenn Sie die Aufgabe Schwachstellen schließen erstellt haben, müssen Sie die in den Aufgabeneinstellungen aufgelisteten Programm-Updates manuell angeben.

Software-Schwachstellen mithilfe des Assistenten für das Schließen von Schwachstellen schließen

Der Assistent für das Schließen von Schwachstellen ist nur im Rahmen der Lizenz für Schwachstellen- und Patch-Management verfügbar.

So schließen Sie Software-Schwachstellen mithilfe des Assistenten für das Schließen von Schwachstellen:

1. Gehen Sie im Hauptmenü zu **Software-Verwaltung → Patch-Management → Schwachstellen in Programmen**.

   Eine Tabelle mit einer Liste von Schwachstellen in Drittanbieter-Anwendungen, die auf den verwalteten Geräten installiert sind, wird angezeigt.

2. Aktivieren Sie das Kontrollkästchen neben der Schwachstelle, die Sie schließen möchten.

3. Klicken Sie auf **Assistent zum Schließen von Schwachstellen starten**.

   Die Schaltfläche ist deaktiviert, wenn Sie mehr als eine Schwachstelle auswählen.

Der Assistent für das Schließen von Schwachstellen wird geöffnet. Die Liste der vorhandenen Aufgaben wird angezeigt. Diese Liste kann die folgenden Aufgabentypen enthalten:

- Erforderliche Updates installieren und Schwachstellen schließen
- Schwachstellen schließen

Sie können die Aufgabe Schwachstellen schließen nicht ändern, um neue Updates zu installieren. Um neue Updates zu installieren, können Sie nur die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen verwenden.

4. Wenn der Assistent nur die Aufgaben anzeigen soll, mit denen die von Ihnen ausgewählte Schwachstelle geschlossen werden kann, aktivieren Sie die Option **Nur Aufgaben anzeigen, die diese Schwachstelle schließen**.

5. Führen Sie eine der folgenden Aktionen aus:

   - Um eine Aufgabe zu starten, aktivieren Sie das Kontrollkästchen neben dem Aufgabennamen und klicken auf **Starten**.

     Es sind keine weiteren Aktionen erforderlich. Sie können den Assistenten schließen. Die Aufgabe wird im Hintergrundmodus durchgeführt.

   - So fügen Sie zu einer bestehenden Aufgabe des Typs Erforderliche Updates installieren und Schwachstellen schließen eine neue Regel hinzu:

     a. Aktivieren Sie das Kontrollkästchen neben dem Aufgabennamen und klicken Sie auf **Regel hinzufügen**.

     > Die Schaltfläche **Regel hinzufügen** ist deaktiviert, wenn Sie mehr als eine Aufgabe auswählen.

     Für die Aufgabe Schwachstellen schließen können Sie keine Regel hinzufügen. Wenn Sie eine Aufgabe des Typs Schwachstellen schließen auswählen, wird die folgende Meldung angezeigt: "Verwenden Sie die Aufgabe 'Erforderliche Updates installieren und Schwachstellen schließen', um Updates zu installieren."

     b. Konfigurieren Sie auf der folgenden Seite die neue Regel:

     - **Regel zum Schließen aller Schwachstellen der ausgewählten Signifikanz**

       Manchmal können sich Programm-Updates negativ auf die Benutzererfahrung eines Programms auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

       Wenn diese Option aktiviert ist, beheben die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als die Signifikanz des ausgewählten Updates (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht behoben.

       Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

       Diese Option ist standardmäßig deaktiviert.

     - **Regel zum Schließen von Schwachstellen mithilfe von Updates des gleichen Typs wie das für die ausgewählte Schwachstelle empfohlene Update**

       Diese Regel wird nur für Schwachstellen in Software von Microsoft angezeigt.

- **Regel zum Schließen von Schwachstellen in Anwendungen des ausgewählten Anbieters**

  Diese Regel wird nur für Schwachstellen in Drittanbieter-Anwendungen angezeigt.

- **Regel zum Schließen von Schwachstellen in allen Versionen der ausgewählten Anwendung**

  Diese Regel wird nur für Schwachstellen in Drittanbieter-Software angezeigt.

- **Regel zum Schließen der ausgewählten Schwachstelle**

- **Updates zum Schließen der ausgewählten Schwachstelle freigeben**

  Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

  Diese Option ist standardmäßig deaktiviert.

c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

Das Fenster mit den Aufgabeneigenschaften wird geöffnet. Die neue Regel wurde den Aufgabeneigenschaften hinzugefügt. Sie können die Regel oder andere Aufgabeneigenschaften anzeigen und anpassen. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

- So erstellen Sie eine Aufgabe:

a. Klicken Sie auf **Neue Aufgabe**.

b. Konfigurieren Sie auf der sich öffnenden Seite die neue Regel:

- **Regel zum Schließen aller Schwachstellen der ausgewählten Signifikanz**

  Manchmal können sich Programm-Updates negativ auf die Benutzererfahrung eines Programms auswirken. In solchen Fällen können Sie festlegen, nur jene Updates zu installieren, die für den Betrieb der Software kritisch sind, und andere Updates zu überspringen.

  Wenn diese Option aktiviert ist, beheben die Updates nur jene Schwachstellen, für welche die von Kaspersky festgelegte Signifikanz gleich oder höher ist als die Signifikanz des ausgewählten Updates (**Mittel**, **Hoch** oder **Kritisch**). Schwachstellen mit einer Signifikanz, die unter dem ausgewählten Wert liegt, werden nicht behoben.

  Wenn diese Option deaktiviert ist, schließen die Updates alle Schwachstellen unabhängig von deren Signifikanz.

  Diese Option ist standardmäßig deaktiviert.

- **Regel zum Schließen von Schwachstellen mithilfe von Updates des gleichen Typs wie das für die ausgewählte Schwachstelle empfohlene Update**

  Diese Regel wird nur für Schwachstellen in Software von Microsoft angezeigt.

- **Regel zum Schließen von Schwachstellen in Anwendungen des ausgewählten Anbieters**

  Diese Regel wird nur für Schwachstellen in Drittanbieter-Anwendungen angezeigt.

- **Regel zum Schließen von Schwachstellen in allen Versionen der ausgewählten Anwendung**

  Diese Regel wird nur für Schwachstellen in Drittanbieter-Software angezeigt.

- **Regel zum Schließen der ausgewählten Schwachstelle**

- **Updates zum Schließen der ausgewählten Schwachstelle freigeben**

Das ausgewählte Update wird zur Installation freigegeben. Aktivieren Sie diese Option, wenn einige übernommene Regeln zur Installation von Updates nur die Installation von bestätigten Updates erlauben.

Diese Option ist standardmäßig deaktiviert.

c. Klicken Sie auf die Schaltfläche **Hinzufügen**.

d. Fahren Sie mit der Erstellung der Aufgabe im Assistent für das Erstellen einer Aufgabe fort.

Die neue Regel, die Sie im Assistenten für das Schließen von Schwachstellen hinzugefügt haben, wird im Schritt **Regeln für die Installation von Updates festlegen** des Assistenten für das Erstellen einer Aufgaben angezeigt. Wenn Sie den Assistenten abschließen, wurde die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen der Aufgabenliste hinzugefügt.

Erstellen der Aufgabe "Schwachstellen schließen"

Mit der Aufgabe *Schwachstellen schließen* können Sie Software-Schwachstellen auf verwalteten Geräten beheben. Sie können Schwachstellen in Drittanbieter-Programmen, einschließlich der Software von Microsoft, schließen.

Sie können die Aufgabe *Schwachstellen schließen* nur für Windows-Geräte erstellen. Sie können diese Aufgabe nicht für Geräte mit anderen Betriebssystemen erstellen.

Sie können neue Aufgaben vom Typ *Schwachstellen schließen* nur dann erstellen, wenn Sie über die Lizenz für das Schwachstellen- und Patch-Management verfügen.

Um neue Schwachstellen zu schließen, können Sie diese Schwachstellen zu einer vorhandenen Aufgabe des Typs *Schwachstellen schließen* hinzufügen. Wir empfehlen jedoch die Verwendung der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* anstelle der Aufgabe *Schwachstellen schließen*. Mit der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* können Sie automatisch mehrere Updates installieren und mehrere Schwachstellen nach benutzerdefinierten Regeln beheben.

Eine Benutzerinteraktion ist möglicherweise erforderlich, wenn Sie ein Drittanbieter-Programm aktualisieren oder auf einem verwalteten Gerät eine Schwachstelle in einem Drittanbieter-Programm beheben. Beispielsweise kann der Benutzer aufgefordert werden, das Drittanbieter-Programm zu schließen, wenn es gerade geöffnet ist.

So erstellen Sie die Aufgabe Schwachstellen schließen:

1. Wechseln Sie im Hauptmenü zu **Aufgaben**.

   Alternativ können Sie diese Aufgabe auch im Eigenschaftenfenster des Geräts auf der Registerkarte **Aufgaben** erstellen.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Klicken Sie auf **Weiter**, um den Schritten des Assistenten zu folgen.

3. Wählen Sie in der Dropdown-Liste **Anwendung** die Option "Kaspersky Security Center" aus.

4. Wählen Sie in der Liste **Aufgabentyp** den Typ **Schwachstellen schließen** aus.

5. Geben Sie im Feld **Aufgabenname** den Namen der neuen Aufgabe an.

   Der Aufgabenname darf nicht mehr als 100 Zeichen umfassen und darf keine Sonderzeiten ("*<>?\:|) enthalten.

6. Wählen Sie die Geräte, denen die Aufgabe zugewiesen werden soll.

   Wechseln Sie zum nächsten Schritt des Assistenten.

7. Klicken Sie auf **Hinzufügen**.

   Die Liste der Schwachstellen wird geöffnet.

8. Aktivieren Sie in der Liste der Schwachstellen die Kontrollkästchen neben den Schwachstellen, die Sie schließen möchten, und klicken Sie anschließend auf **OK**.

   Schwachstellen in der Software von Microsoft besitzen normalerweise empfohlene Korrekturen. Für sie sind keine zusätzlichen Aktionen erforderlich.

   Bei Schwachstellen in der Software anderer Hersteller müssen Sie zunächst eine individuelle Korrektur für jede Schwachstelle angeben, die Sie schließen möchten. Danach können Sie diese Schwachstellen zu der Aufgabe *Schwachstellen schließen* hinzufügen.

   Gehen Sie zum nächsten Schritt des Assistenten.

9. Geben Sie die Einstellungen für den Neustart des Betriebssystems an:

   - **Gerät nicht neu starten**

     Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Zum Abschließen des Vorgangs müssen Sie das Gerät neu starten (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten). Die Informationen über einen erforderlichen Neustart werden in den Ergebnissen der Aufgabenausführung und im Status des Geräts gespeichert. Diese Variante eignet sich für Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreier Betrieb wichtig ist.

   - **Gerät neu starten**

     Client-Geräte werden immer automatisch neu gestartet, wenn zum Abschließen des Vorgangs ein Neustart erforderlich ist. Diese Variante eignet sich für Aufgaben auf Geräten, deren Betrieb regelmäßige Pausen vorsieht (z. B. zum Herunterfahren oder Neustart).

   - **Benutzer fragen**

     Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und der Benutzer wird aufgefordert, das Gerät manuell neu zu starten. Für diese Variante können einige erweiterte Einstellungen festgelegt werden: Text der Nachricht an den Benutzer, Anzeigehäufigkeit der Nachricht und Zeitspanne, nach der ein Neustart zwangsläufig (ohne Bestätigung des Benutzers) ausgeführt wird. Diese Option eignet sich am besten für Workstations, auf denen Benutzer in der Lage sein müssen, den passenden Zeitpunkt für einen Neustart auszuwählen.

     Diese Option ist standardmäßig ausgewählt.

   - **Aufforderung wiederholen alle (Min.)**

     Wenn diese Option aktiviert ist, fordert die Anwendung den Benutzer im festgelegten Zeitabstand auf, das Betriebssystem neu zu starten.

     Diese Option ist standardmäßig aktiviert. Das Standardintervall beträgt 5 Minuten. Ein Wert zwischen 1 Minute und 1.440 Minuten ist möglich.

     Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten nach (Min.)**

  Nachdem der Benutzer aufgefordert wurde, erzwingt das Programm den Neustart des Betriebssystems nach Ablauf der festgelegten Zeitspanne.

  Diese Option ist standardmäßig aktiviert. Die Standardverzögerung beträgt 30 Minuten. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

- **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können einen Neustart des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einem Textverarbeitungsprogramm bearbeitet wird und nicht gespeichert wurde, verhindert dieses Programm einen Neustart des Geräts.

  Wenn diese Option aktiviert ist, werden solche Programme auf einem gesperrten Gerät zwangsweise geschlossen, bevor das Gerät neu gestartet wird. Dadurch können Benutzer nicht gespeicherte Änderungen verlieren.

  Wenn diese Option deaktiviert ist, wird ein gesperrtes Gerät nicht neu gestartet. Der Aufgabenstatus auf diesem Gerät weist darauf hin, dass ein Neustart des Geräts erforderlich ist. Benutzer müssen alle Anwendungen, die auf gesperrten Geräten laufen, manuell schließen und diese Geräte neu starten.

  Diese Option ist standardmäßig deaktiviert.

Gehen Sie zum nächsten Schritt des Assistenten.

10. Legen Sie die Benutzerkonto-Einstellungen fest:

    - **Standardbenutzerkonto**

      Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, wie die Anwendung, durch welche diese Aufgabe ausgeführt wird.

      Diese Variante ist standardmäßig ausgewählt.

    - **Benutzerkonto festlegen**

      Füllen Sie die Felder **Benutzerkonto** und **Kennwort** aus. Geben Sie hier die Details für das Benutzerkonto an, unter dem die Aufgabe ausgeführt werden soll. Das Benutzerkonto muss über die für diese Aufgabe erforderlichen Rechte verfügen.

    - **Benutzerkonto**

      Benutzerkonto, unter dem die Aufgabe ausgeführt wird.

    - **Kennwort**

      Kennwort des Benutzerkontos, unter dem die Aufgabe ausgeführt wird.

11. Aktivieren Sie beim Schritt **Erstellung der Aufgabe abschließen** des Assistenten die Option **Nach Abschluss der Erstellung Aufgabendetails öffnen**, um die standardmäßigen Aufgabeneinstellungen zu ändern.

    Wenn Sie diese Option nicht aktivieren, wird die Aufgabe mit den Standardeinstellungen erstellt. Sie können die Standardeinstellungen später ändern.

12. Klicken Sie auf die Schaltfläche **Fertigstellen**.

    Der Assistent erstellt die Aufgabe. Wenn Sie die Option Nach **Nach Abschluss der Erstellung Aufgabendetails öffnen** haben, wird das Fenster mit Aufgabeneigenschaften automatisch geöffnet. In diesem Fenster können Sie die allgemeinen Aufgabeneinstellungen angeben und bei Bedarf die Einstellungen ändern, die bei der Aufgabenerstellung festgelegt wurden.

Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Aufgabenliste auf den Namen der erstellten Aufgabe klicken.

Die Aufgabe wurde erstellt, konfiguriert und wird in der Aufgabenliste unter **Aufgaben** angezeigt.

13. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf **Starten**.

    Auf der Registerkarte **Zeitplan** im Eigenschaftenfenster der Aufgabe können Sie auch einen Zeitplan für den Aufgabenstart festlegen.

    Eine genaue Beschreibung der Einstellungen für den Start nach Zeitplan finden Sie in den allgemeinen Aufgabeneinstellungen.

Nach Abschluss der Aufgabe wurden die ausgewählten Schwachstellen geschlossen.

Auswählen von Benutzerkorrekturen für Schwachstellen in Programmen von Drittanbietern

Zur Verwendung der Aufgabe *Schwachstellen schließen* müssen Sie die Programm-Updates manuell angeben, mit denen die in den Aufgabeneinstellungen angegeben Schwachstellen in den Drittanbieter-Programmen behoben werden sollen. Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für Software von Microsoft und die individuelle Korrekturen für andere Drittanbieter-Programme.

Individuelle Korrekturen sind Programm-Updates, die ein Administrator manuell zur Installation festlegt, um Schwachstellen zu schließen.

So wählen Sie individuelle Korrekturen für Schwachstellen in Drittanbieter-Programmen aus:

1. Gehen Sie im Hauptmenü zu **Software-Verwaltung → Patch-Management → Schwachstellen in Programmen**.

   Eine Tabelle mit der Liste von Schwachstellen in Drittanbieter-Anwendungen, die auf den verwalteten Geräten installiert sind, wird angezeigt.

2. Klicken Sie in der Liste der Software-Schwachstellen auf den Link mit dem Namen der Software-Schwachstelle, für die Sie eine benutzerdefinierte Korrektur angeben möchten.

   Das Eigenschaftenfenster der ausgewählten Schwachstelle wird geöffnet.

3. Wählen Sie im linken Bereich den Abschnitt **Benutzerdefinierte und andere Patches** aus.

   Die Liste der individuellen Korrekturen für die ausgewählte Software-Schwachstelle wird angezeigt.

4. Klicken Sie auf **Hinzufügen**.

   Eine Liste der verfügbaren Installationspakete wird angezeigt. Die Liste der angezeigten Installationspakete entspricht der Liste unter **Software-Verwaltung → Installationspakete**.

   Wenn Sie kein Installationspaket erstellt haben, das eine individuelle Korrektur für die ausgewählte Schwachstelle enthält, können Sie das Paket jetzt erstellen. Klicken Sie dazu auf die Schaltfläche **Neu** und folgen Sie den Schritten des Assistenten für neue Installationspakete.

5. Wählen Sie ein Installationspaket (bzw. Pakete) aus, das eine benutzerdefinierte Korrektur (bzw. individuelle Korrekturen) für die ausgewählte Schwachstelle enthält.

6. Klicken Sie auf **Speichern**.

   Die Installationspakete, die individuelle Korrekturen für die Software-Schwachstelle enthalten, sind nun angegeben. Wenn Sie die Aufgabe *Schwachstellen schließen* starten, wird das Installationspaket installiert und die Software-Schwachstelle wird behoben.

Anzeigen von Informationen zu Schwachstellen in Programmen, die auf allen verwalteten Geräten erkannt wurden

Nachdem Sie die Software auf verwalteten Geräten auf Schwachstellen untersucht haben, können Sie die Liste der erkannten Software-Schwachstellen anzeigen. Wenn Sie die Aufgabe für die Hierarchie der Administrationsserver ausführen, können Sie die Liste der verwalteten Geräte mit erkannten Schwachstellen nur für den ausgewählten Administrationsserver anzeigen.

Sie können auch einen Bericht über Schwachstellen erstellen und anzeigen.

So zeigen Sie eine Liste mit Software-Schwachstellen an, die auf allen verwalteten Geräten erkannt wurden:

Gehen Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

Die Liste der Software-Schwachstellen, die auf Client-Geräten erkannt wurden, wird angezeigt.

So passen Sie die Liste der Software-Schwachstellen an:

Klicken Sie auf das **Filter**-Symbol ( ) oben rechts in der Liste mit den Software-Schwachstellen und wählen Sie den gewünschten Filter aus. Sie können auch einen voreingestellten Filter aus der Dropdown-Liste **Vordefinierte Filter** oberhalb der Liste mit Software-Schwachstellen auswählen.

Sie können genaue Informationen über eine beliebige Schwachstelle aus der Liste entnehmen.

So rufen Sie Informationen über eine Software-Schwachstelle ab:

Klicken Sie in der Liste mit den Software-Schwachstellen auf den Link mit dem Namen der Schwachstelle.

Das Eigenschaftenfenster der Software-Schwachstelle wird geöffnet.

Anzeigen von Informationen zu Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden

Sie können Informationen zu Software-Schwachstellen, die auf dem ausgewählten verwalteten Windows-Gerät erkannt wurden, anzeigen.

So zeigen Sie die Liste der Software-Schwachstellen an, die auf dem ausgewählten verwalteten Gerät gefunden wurden:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung → Assets (Geräte)**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des Geräts, für das Sie erkannte Software-Schwachstellen anzeigen möchten.

   Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.

3. Klicken Sie im Eigenschaftenfenster des ausgewählten Geräts auf die Registerkarte **Erweitert**.

4. Wählen Sie im linken Fensterbereich den Abschnitt **Schwachstellen in Programmen** aus.

Die Liste der Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden, wird angezeigt.

So zeigen Sie die Eigenschaften der ausgewählten Schwachstelle an:

Klicken Sie in der Liste der Software-Schwachstellen auf den Link mit dem Namen der Schwachstelle.

Das Eigenschaftenfenster der ausgewählten Schwachstelle wird geöffnet.

Anzeigen von Statistiken zu Schwachstellen auf verwalteten Geräten

Sie können eine Statistik für jede Software-Schwachstelle auf verwalteten Geräten anzeigen. Die Statistik wird als Diagramm angezeigt. Das Diagramm enthält die Anzahl der Geräte mit den folgenden Statusvarianten:

- *Ignoriert auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie in den Eigenschaften der Schwachstelle manuell die Option zum Ignorieren der Schwachstelle festgelegt haben.
- *Geschlossen auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn die Aufgabe zum Schließen der Schwachstelle erfolgreich abgeschlossen wurde.
- *Korrektur geplant auf <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie die Aufgabe zum Schließen der Schwachstelle erstellt haben, die Aufgabe jedoch noch nicht ausgeführt wurde.
- *Patch angewendet auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie ein Programm-Update zur Behebung der Schwachstelle manuell ausgewählt haben, die Schwachstelle jedoch dadurch nicht geschlossen wurde.
- *Korrektur erforderlich auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn die Schwachstelle nur auf einigen der verwalteten Geräten geschlossen wurde und auf den anderen verwalteten Geräten noch geschlossen werden muss.

So zeigen Sie die Statistik über Schwachstelle auf einem verwalteten Gerät an:

1. Wechseln Sie im Hauptmenü zu **Vorgänge → Patch-Management → Schwachstellen in Programmen**.

   Die Seite enthält eine Liste der Software-Schwachstellen, die auf den verwalteten Geräten erkannt wurden.

2. Aktivieren Sie das Kontrollkästchen neben einer Schwachstelle.

3. Klicken Sie auf **Statistik zu Schwachstellen auf Geräten**.

   Die Schaltfläche **Statistik zu Schwachstellen auf Geräten** ist deaktiviert, wenn Sie mehr als eine Schwachstelle auswählen.

Ein Diagramm mit den Statusvarianten der Schwachstellen wird angezeigt. Wenn Sie auf einen Status klicken, wird eine Liste der Geräte geöffnet, auf denen die Schwachstelle den ausgewählten Status hat.

Exportieren der Liste von Schwachstellen in Programmen in eine Datei

Sie können die angezeigte Liste der Schwachstellen als csv- oder txt-Datei herunterladen. Sie können diese Dateien an Ihren Information Security Manager senden oder für statistische Zwecke speichern.

So exportieren Sie eine Liste der Software-Schwachstellen, die auf allen verwalteten Geräten erkannt wurden, in eine Textdatei:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

   Eine Liste der Software-Schwachstellen, die auf verwalteten Geräten gefunden wurden, wird angezeigt.

   Standardmäßig werden nur jene Schwachstellen exportiert, die auf der aktuellen Seite zu sehen sind.

   Wenn Sie nur ausgewählte Schwachstellen exportieren möchten, aktivieren Sie die Kontrollkästchen neben diesen Schwachstellen.

2. Klicken Sie auf **In txt-Datei exportieren** oder **In csv-Datei exportieren**, je nachdem, welches Format Sie bevorzugen. Wenn keine dieser Schaltflächen sichtbar ist, klicken Sie auf die Schaltfläche mit den drei Punkten und wählen Sie anschließend in der Dropdown-Liste die gewünschte Option aus.

Eine Datei mit der Liste der Software-Schwachstellen wird auf Ihr Gerät heruntergeladen.

So zeigen Sie die Liste der Software-Schwachstellen an, die auf dem ausgewählten verwalteten Gerät gefunden wurden:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des Geräts, für das Sie erkannte Software-Schwachstellen anzeigen möchten.

   Das Eigenschaftenfenster des ausgewählten Geräts wird angezeigt.

3. Klicken Sie im Eigenschaftenfenster des ausgewählten Geräts auf die Registerkarte **Erweitert**.

4. Wählen Sie im linken Fensterbereich den Abschnitt **Schwachstellen in Programmen** aus.

Die Liste der Software-Schwachstellen, die auf dem ausgewählten verwalteten Gerät erkannt wurden, wird angezeigt.

Standardmäßig werden nur jene Schwachstellen exportiert, die auf der aktuellen Seite zu sehen sind.

Wenn Sie nur ausgewählte Schwachstellen exportieren möchten, aktivieren Sie die Kontrollkästchen neben diesen Schwachstellen.

1. Klicken Sie auf **In txt-Datei exportieren** oder **In csv-Datei exportieren**, je nachdem, welches Format Sie bevorzugen. Wenn keine dieser Schaltflächen sichtbar ist, klicken Sie auf die Schaltfläche mit den drei Punkten und wählen Sie anschließend in der Dropdown-Liste die gewünschte Option aus.

Eine Datei mit der Liste der Software-Schwachstellen wird auf Ihr Gerät heruntergeladen.

Ignorieren von Schwachstellen in Programmen

Sie können Korrekturen für Software-Schwachstellen ignorieren. Gründe für das Ignorieren von Schwachstellen in Programmen können sein:

- Sie betrachten die Software-Schwachstelle nicht als kritisch für Ihr Unternehmen.
- Sie vermuten, dass durch das Schließen von Software-Schwachstellen die Daten des Programms beschädigt werden können, welches das Schließen von Schwachstellen erforderlich macht.
- Sie sind sicher, dass die Software-Schwachstelle keine Gefahr für das Netzwerk Ihres Unternehmens darstellt, da Sie andere Maßnahmen ergriffen haben, um Ihre verwalteten Geräte zu schützen.

Sie können eine Software-Schwachstelle auf allen verwalteten Geräten oder nur auf ausgewählten verwalteten Geräten ignorieren.

So ignorieren Sie eine Schwachstelle im Programm auf allen verwalteten Geräten:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

   Eine Liste der Software-Schwachstellen, die auf verwalteten Geräten gefunden wurden, wird angezeigt.

2. Klicken Sie in der Liste der Software-Schwachstellen auf den Link mit dem Namen der Schwachstelle, die Sie ignorieren möchten.

   Das Eigenschaftenfenster der Software-Schwachstelle wird geöffnet.

3. Aktivieren Sie auf der Registerkarte **Allgemein** die Option **Schwachstelle ignorieren**.

4. Klicken Sie auf die Schaltfläche **Speichern**.

   Das Eigenschaftenfenster der Software-Schwachstelle wird geschlossen.

Die Software-Schwachstelle wird auf allen verwalteten Geräten ignoriert.

So ignorieren Sie eine Software-Schwachstelle auf einem ausgewählten verwalteten Gerät:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des Geräts, auf dem Sie eine Software-Schwachstelle ignorieren möchten.

   Das Eigenschaftenfenster für das Gerät wird geöffnet.

3. Wählen Sie im Eigenschaftenfenster des Geräts die Registerkarte **Erweitert** aus.

4. Wählen Sie im linken Bereich den Abschnitt **Schwachstellen in Programmen** aus.

   Die Liste der Software-Schwachstellen, die auf dem Gerät erkannt wurden, wird angezeigt.

5. Wählen Sie in der Liste der Software-Schwachstellen jene aus, die Sie auf dem ausgewählten Gerät ignorieren möchten.

   Das Fenster mit den Eigenschaften der Schwachstelle im Programm öffnet sich.

6. Aktivieren Sie im Eigenschaftenfenster der Software-Schwachstelle auf der Registerkarte **Allgemein** die Option **Schwachstelle ignorieren**.

7. Klicken Sie auf die Schaltfläche **Speichern**.

   Das Fenster mit den Eigenschaften der Schwachstelle im Programm schließt sich.

8. Schließen Sie das Eigenschaftenfenster des Geräts.

Die Software-Schwachstelle wird auf dem ausgewählten Gerät ignoriert.

Die ignorierte Software-Schwachstelle wird im Rahmen der Aufgabe *Schwachstellen schließen* oder *Erforderliche Updates installieren und Schwachstellen schließen* nicht behoben. Mithilfe eines Filters können Sie ignorierte Software-Schwachstellen aus der Liste der Schwachstellen ausschließen.

Erstellen eines Installationspakets eines Drittanbieterprogramms aus der Kaspersky-Datenbank

Mit Kaspersky Security Center Web Console können Sie Installationspakete erstellen, um eine Remote-Installation von Drittanbieter-Anwendungen durchzuführen. Solche Drittanbieter-Anwendungen sind in einer dedizierten Kaspersky-Datenbank enthalten. Diese Datenbank wird automatisch erstellt, wenn Sie die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* starten.

> Sie können nur dann ein Installationspaket für eine Drittanbieter-Anwendung aus der Kaspersky-Datenbank erstellen, wenn Sie über eine Lizenz für das Schwachstellen- und Patch-Management verfügen.

So erstellen Sie ein Installationspaket für eine Drittanbieter-Anwendung aus der Kaspersky-Datenbank:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung** → **Installationspakete**.

2. Klicken Sie auf **Hinzufügen**.

   Der Assistent für das Erstellen eines Installationspakets wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.

3. Wählen Sie die Option **Anwendung aus der Kaspersky-Datenbank auswählen, um ein Installationspaket zu erstellen**.

   > Diese Option ist nur im Rahmen der Lizenz für Schwachstellen- und Patch-Management verfügbar.

   Gehen Sie zum nächsten Schritt des Assistenten.

4. Wählen Sie das Programm aus, für das Sie ein Installationspaket erstellen möchten.

   Gehen Sie zum nächsten Schritt des Assistenten.

5. Wählen Sie die erforderliche Sprachversion in der Dropdown-Liste aus und klicken Sie dann auf Weiter.

   Dieser Schritt wird nur angezeigt, wenn die Anwendung mehrere Sprachen zur Auswahl bietet.

6. Wenn Sie im Schritt **Lizenzverträge und Datenschutzrichtlinien** des Assistenten aufgefordert werden, einen Lizenzvertrag für die Installation zu akzeptieren, gehen Sie wie folgt vor:

   a. Klicken Sie auf den Link **Anzeigen**, um den Lizenzvertrag auf der Website des Anbieters zu lesen oder die Updates mit der Lizenz anzuzeigen.

   b. Aktivieren Sie das Kontrollkästchen **Ich bestätige, dass ich die Bestimmungen und Bedingungen dieses Endbenutzer-Lizenzvertrags vollständig gelesen habe, und sie verstehe und akzeptiere**.

   c. Klicken Sie auf **Alle akzeptieren**, um alle Lizenzverträge und Datenschutzrichtlinien zu akzeptieren, die in der Liste angezeigt werden.

7. Geben Sie bei Schritt **Name des neuen Installationspakets** des Assistenten im Feld **Paketname** einen Namen für das Installationspaket ein und klicken dann auf **Weiter**.

   Das neu erstellte Installationspaket wird auf den Administrationsserver hochgeladen. Der Assistent für das Erstellen eines Installationspakets zeigt eine Nachricht darüber an, dass das Installationspaket erfolgreich erstellt wurde.

8. Klicken Sie auf **Fertigstellen**.

Das neu erstellte Installationspaket wird in der Liste der Installationspakete angezeigt. Sie können dieses Paket auswählen, wenn Sie die Aufgabe *Remote-Installation einer Anwendung* erstellen oder anpassen.

Sie können die Aufgabe *Remote-Installation einer Anwendung* nur dann unter Verwendung des Installationspakets einer Drittanbieter-Anwendung aus der Kaspersky-Datenbank erstellen und ändern, wenn Sie über eine Lizenz für das Schwachstellen- und Patch-Management verfügen.

Anzeigen und anpassen der Einstellungen von einem Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank

Wenn Sie bereits Installationspakete für Drittanbieter-Anwendungen erstellt haben, die in der Kaspersky-Datenbank gelistet sind, können Sie die Einstellungen dieser Pakete später anzeigen und anpassen.

Das Anpassen der Einstellungen eines Installationspakets einer Drittanbieter-Anwendung steht nur im Rahmen der Lizenz für das Schwachstellen- und Patch-Management zur Verfügung.

Um die Einstelllungen eines Installationspakets einer Drittanbieter-Anwendung aus der Kaspersky-Datenbank anzuzeigen und anzupassen:

1. Wechseln Sie im Hauptmenü zu **Software-Verwaltung** → **Installationspakete**.
2. Klicken Sie in der Liste der Installationspakete auf den Namen des gewünschten Installationspakets.
   Das Eigenschaftenfenster wird geöffnet.
3. Ändern Sie bei Bedarf die Einstellungen.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Die geänderten Einstellungen werden gespeichert.

Einstellungen eines Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank

Die Einstellungen für das Installationspaket einer Drittanbieter-Anwendung sind auf den folgenden Registerkarten angeordnet:

> Nicht alle der unten aufgeführten Einstellungen werden standardmäßig angezeigt. Sie können die gewünschten Spalten hinzufügen, indem Sie auf die Schaltfläche **Filter** klicken und anschließend die erforderlichen Spaltennamen aus der Liste auswählen.

- Registerkarte **Allgemein**:
  - Eingabefeld, das den Namen des Installationspakets enthält und manuell angepasst werden kann
  - **Anwendung**

    Name der Drittanbieter-Anwendung, für welche das Installationspaket erstellt wurde.
  - **Version**

    Versionsnummer der Drittanbieter-Anwendung, für welche das Installationspaket erstellt wurde.
  - **Größe**

    Größe des Drittanbieter-Installationspakets (in Kilobyte).
  - **Erstellt**

    Datum und Uhrzeit der Erstellung des Drittanbieter-Installationspakets.
  - **Pfad**

    Pfad des Netzwerkordners, in dem sich das Drittanbieter-Installationspaket befindet.

- Registerkarte **Installationsreihenfolge**:
  - **Erforderliche allgemeine Systemkomponenten installieren**

    Wenn diese Option aktiviert ist, installiert die Anwendung vor der Installation eines Updates automatisch alle allgemeinen Systemkomponenten (erforderlichen Komponenten), die für die Installation des Updates erforderlich sind. Diese erforderlichen Komponenten können beispielsweise Updates des Betriebssystems sein.

    Wenn diese Option deaktiviert ist, müssen Sie die erforderlichen Komponenten möglicherweise manuell installieren.

    Diese Option ist standardmäßig deaktiviert.

  - Eine Tabelle, welche die Update-Eigenschaften enthält und die folgenden Spalten enthält:
    - **Name**

      Name des Updates.

    - **Beschreibung**

      Beschreibung des Updates.

    - **Quelle**

      Quelle des Updates, d. h. ob das Update von Microsoft oder von einem anderen Drittanbieter veröffentlicht wurde.

    - **Typ**

      Typ des Updates, d. h. ob es für einen Treiber oder für ein Programm vorgesehen ist.

    - **Kategorie**

      Die für Microsoft-Updates angegebene Kategorie des Windows Server Update-Dienstes (WSUS) (Kritische Updates, Definitions-Updates, Treiber, Funktionspakete, Sicherheits-Updates, Service Packs, Tools, Update-Rollups, Updates oder Upgrades).

    - **Ereigniskategorie nach MSRC**

      Die durch das Microsoft Security Response Center (MSRC) definierte Ereigniskategorie des Updates.

    - **Ereigniskategorie**

      Die durch Kaspersky definierte Ereigniskategorie des Updates.

    - **Ereigniskategorie des Patches**

      Ereigniskategorie eines Patches, wenn dieser für eine Kaspersky-Anwendung vorgesehen ist.

    - **Artikel**

      ID des Artikels, der das Update in der Wissensdatenbank beschreibt.

    - **Bulletin**

      ID des Sicherheitsbulletins mit einer Beschreibung des Updates.

- **Nicht zur Installation bestimmt (neue Version)**

  Gibt an, ob das Update den Status "Nicht zur Installation bestimmt" besitzt.

- **Bestimmt für die Installation**

  Gibt an, ob das Update den Status "Für die Installation bestimmt" besitzt.

- **Wird installiert**

  Gibt an, ob das Update den Status "Wird installiert" besitzt.

- **Installiert**

  Gibt an, ob das Update den Status "Installiert" besitzt.

- **Fehlgeschlagen**

  Gibt an, ob das Update den Status "Fehlgeschlagen" besitzt.

- **Neustart erforderlich**

  Gibt an, ob das Update den Status "Neustart erforderlich" besitzt.

- **Registriert**

  Gibt den Zeitpunkt (Datum und Uhrzeit) an, zu dem das Update registriert wurde.

- **Wird im interaktiven Modus installiert**

  Gibt an, ob das Update während der Installation eine Benutzerinteraktion erfordert.

- **Status der Update-Genehmigung**

  Gibt an, ob das Update zur Installation genehmigt wurde.

- **Revision**

  Gibt die aktuelle Revisionsnummer des Updates an.

- **Update-ID**

  Gibt die Update-ID an.

- **Anwendungsversion**

  Gibt die Versionsnummer an, auf die das Programm aktualisiert wird.

- **Ersetzt**

  Gibt ein oder mehrere andere Updates an, die dieses Update ersetzen können.

- **Ersetzend**

  Gibt ein oder mehrere Updates an, die durch dieses Update ersetzt werden können.

- **Sie müssen die Bedingungen des Lizenzvertrags akzeptieren**

  Gibt an, ob das Update das Akzeptieren des Endbenutzer-Lizenzvertrags (EULA) erfordert.

- **URL der Beschreibung**

  Gibt den Namen des Update-Herstellers an.

- **Anwendungsfamilie**

  Gibt den Namen der Programmfamilie an, zu welcher dieses Update gehört.

- **Anwendung**

  Gibt den Namen des Programms an, zu dem dieses Update gehört.

- **Lokalisierungssprache**

  Gibt die Sprache der Update-Lokalisierung an.

- **Nicht zur Installation bestimmt (neue Version)**

  Gibt an, ob das Update den Status "Nicht zur Installation bestimmt (neue Version)" besitzt.

- **Erforderliche Komponenten müssen installiert werden**

  Gibt an, ob das Update den Status "Erforderliche Komponenten müssen installiert werden" besitzt.

- **Download-Modus**

  Gibt den Modus des Update-Downloads an.

- **Ist ein Patch**

  Gibt an, ob das Update ein Patch ist.

- **Nicht installiert**

  Gibt an, ob das Update den Status "Nicht installiert" besitzt.

- **Erstellt**

- Registerkarte **Einstellungen** welche die Einstellungen des Installationspakets mit den Namen, Beschreibungen und Werten anzeigt, die als Befehlszeilenparameter während der Installation verwendet werden. Wenn ein Paket nicht über derartige Einstellungen verfügt, wird ein entsprechender Hinweis angezeigt. Die Werte dieser Einstellungen können angepasst werden.

- Registerkarte **Revisionsverlauf**, welche die Revisionen des Installationspakets enthält und die folgenden Spalten hat:

  - **Revision** – Revisionsnummer des Installationspakets.

  - **Uhrzeit** – Datum und Uhrzeit der Änderung von Einstellungen des Installationspakets.

  - **Benutzer** – Name des Benutzers, der die Einstellungen des Installationspakets geändert hat.

  - **IP-Adresse des Benutzergeräts** – IP-Adresse des Geräts, von dem aus das Objekt geändert wurde.

  - **IP-Adresse der Web Console** – IP-Adresse der Kaspersky Security Center Web Console, mit der das Objekt geändert wurde.

  - **Aktion** – Aktion, die während der Revision mit dem Installationspaket durchgeführt wurden.

- **Beschreibung** – Beschreibung der Revision der am Installationspaket vorgenommenen Änderungen

  Standardmäßig ist die Beschreibung der Revision leer. Um einer Revision eine eine Beschreibung hinzuzufügen, wählen Sie die gewünschte Revision aus und klicken Sie auf die Schaltfläche **Beschreibung bearbeiten**. Geben Sie im folgenden Fenster einen Text zur Beschreibung der Revision ein.

Schließen von Schwachstellen in einem isolierten Netzwerk

In diesem Abschnitt werden die Schritte beschrieben, mit denen Sie Schwachstellen in Drittanbieter-Programmen auf verwalteten Geräten schließen können, die mit Administrationsservern ohne Internetzugang verbunden sind.

Szenario: Beheben von Schwachstellen in Programmen von Drittanbietern in einem isolierten Netzwerk

Sie können Updates installieren und Schwachstellen in Drittanbieter-Programmen beheben, die auf den verwalteten Geräten in einem isolierten Netzwerk installiert sind. Solche Netzwerke umfassen sowohl Administrationsserver als auch die damit verbundenen verwalteten Geräte ohne Internetzugang. Um Schwachstellen in einem solchen Netzwerk zu schließen, benötigen Sie einen Administrationsserver, der mit dem Internet verbunden ist. Wenn der Administrationsserver einen Internetzugang besitzt, können Sie Patches (erforderliche Updates) herunterladen und sie anschließend auf isolierte Administrationsserver übertragen.

> Mittels Kaspersky Security Center können Sie von Softwareherstellern veröffentlichte Updates für Drittanbieter-Programme auf isolierte Administrationsserver herunterladen. Dies gilt jedoch nicht für die Updates der Software von Microsoft.

Weitere Informationen zum Beheben von Schwachstellen in einem isolierten Netzwerk finden Sie in der Beschreibung und im Schema für diesen Vorgang.

Erforderliche Vorrausetzungen

Treffen Sie zuerst die folgenden Voraussetzungen:

1. Weisen Sie ein Gerät für die Verbindung mit dem Internet und das Herunterladen von Patches zu. Dieses Gerät dient als Administrationsserver mit Internetzugang.
2. Installieren Sie Kaspersky Security Center Linux Version 15.1 oder höher auf den folgenden Geräten:
   - Dediziertes Gerät, das als Administrationsserver mit Internetzugang dient
   - Isolierte Geräte, die als Administrationsserver dienen und vom Internet isoliert sind (im Folgenden "isolierte Administrationsserver" genannt)
3. Stellen Sie sicher, dass jeder Administrationsserver über genügend Speicherplatz zum Herunterladen und Speichern von Updates und Patches verfügt.

Schritte

Die Update-Installation und das Beheben von Schwachstellen in Drittanbieter-Programmen auf den verwalteten Geräten der isolierten Administrationsserver umfasst die folgenden Schritte:

1. **Konfiguration des Administrationsservers mit Internetzugang**

   Bereiten Sie Ihren Administrationsserver mit Internetzugang vor, um Anfragen zu erforderlichen Updates für Drittanbieter-Programme zu bearbeiten und Patches herunterzuladen.

2. **Konfiguration der isolierten Administrationsserver**

   Bereiten Sie Ihre isolierten Administrationsserver vor, damit diese regelmäßig Listen mit erforderlichen Updates erstellen können und die Patches anwenden, die vom Administrationsserver mit Internetzugang heruntergeladen wurden. Nach der Konfiguration versuchen die isolierten Administrationsserver nicht mehr, Patches aus dem Internet herunterzuladen. Stattdessen erhalten sie die Updates mithilfe von Patches.

3. **Übertragung von Patches und Installation von Updates auf isolierten Administrationsservern**

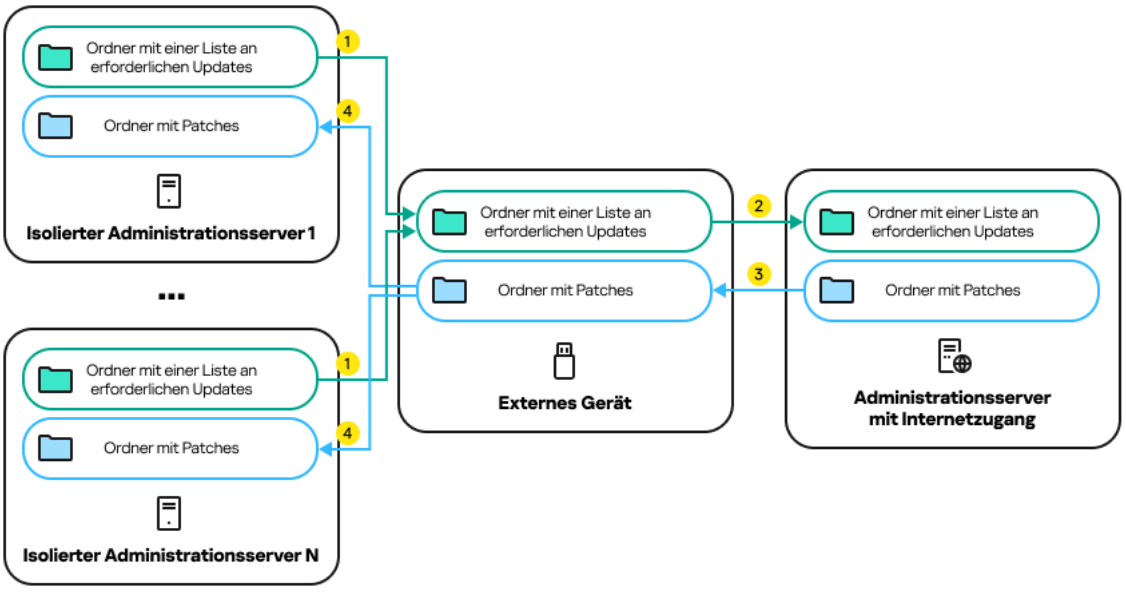
   Nachdem Sie die Konfiguration der Administrationsserver abgeschlossen haben, können Sie die Übertragung der Liste mit erforderlichen Updates und Patches vom Administrationsserver mit Internetzugang an die isolierten Administrationsserver vornehmen. Anschließend werden mithilfe der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* die Updates aus den Patches auf den verwalteten Geräten installiert.

Ergebnisse

Die Updates für Drittanbieter-Programme werden auf isolierte Administrationsserver übertragen und mithilfe von Kaspersky Security Center Linux auf den verbundenen verwalteten Geräten installiert. Es ist ausreichend, die Administrationsserver einmal zu konfigurieren. Anschließend können Sie beliebig oft Updates erhalten, beispielsweise einmal oder mehrmals täglich.

Über das Beheben von Schwachstellen in Programmen von Drittanbietern in einem isolierten Netzwerk

Der Vorgang zum Beheben von Schwachstellen in Drittanbieter-Programmen innerhalb eines isolierten Netzwerks ist in der folgenden Abbildung beschrieben. Sie können diesen Vorgang regelmäßig wiederholen.



Vorgang zur Übertragung von Patches und der Liste mit erforderlichen Updates zwischen dem Administrationsserver mit Internetzugang und den isolierten Administrationsservern

Jeder vom Internet isolierte Administrationsserver (im Folgenden "isolierter Administrationsserver" genannt) erstellt eine Liste der Updates, die auf den verwalteten Geräten installiert werden müssen, die mit diesem Administrationsserver verbunden sind. Diese Liste mit Updates wird in einem bestimmten Ordner in Form von Binärdateien gespeichert. Jede Datei ist nach der ID des Patches benannt, der das erforderliche Update enthält. Daher entspricht jede Datei in der Liste einem bestimmten Patch.

Die Liste der erforderlichen Updates wird über ein externes Gerät vom isolierten Administrationsserver an den angegebenen Administrationsserver mit Internetzugang übertragen. Anschließend lädt der dedizierte Administrationsserver die Patches aus dem Internet herunter und legt sie in einem speziellen Ordner ab.

Nachdem alle Patches heruntergeladen und im angegebenen Ordner abgelegt wurden, werden sie zurück auf alle isolierten Administrationsserver übertragen, von denen eine Liste mit erforderlichen Updates bezogen wurde. Die Patches werden auf allen isolierten Administrationsservern in einem eigens für sie erstellten Ordner gespeichert.

Auf diese Weise führt die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* die Patches aus und installiert die Updates auf den verwalteten Geräten der isolierten Administrationsserver.

Administrationsserver mit Internetzugang konfigurieren, um Schwachstellen in einem isolierten Netzwerk zu schließen

Um das Schließen von Schwachstellen und die Übertragung von Patches innerhalb eines isolierten Netzwerks vorzubereiten, müssen Sie zuerst den Administrationsserver mit Internetzugang konfigurieren und anschließend die isolierten Administrationsserver konfigurieren.

So konfigurieren Sie einen Administrationsserver mit Internetzugang:

1. Erstellen Sie zwei Ordner auf der Festplatte, auf welcher der Administrationsserver installiert ist:

   - Ordner für die Liste mit erforderlichen Updates
   - Ordner für Patches

   Sie können diesen Ordnern beliebige Namen geben.

2. Weisen Sie der Gruppe "KLAdmins" für die erstellten Ordner die Berechtigung **Ändern** zu. Verwenden Sie dazu die Standardverwaltungstools des Betriebssystems.

3. Verwenden Sie das Dienstprogramm "klscflag", um die Pfade zu diesen Ordnern in den Eigenschaften des Administrationsservers anzugeben.

   Öffnen Sie die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

4. Führen Sie in der Befehlszeile die folgenden Befehle aus:

   - Um den Pfad zum Patch-Ordner festzulegen:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<Pfad zum Ordner>"`
   - Um den Pfad zum Ordner für die Liste mit erforderlichen Updates festzulegen:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<Pfad zum Ordner>"`

   Beispiel: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "/OrnderFürPatches"`

5. Verwenden Sie bei Bedarf das Tool "klscflag", um anzugeben, wie oft der Administrationsserver nach neuen Patch-Anforderungen suchen soll:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <Wert in Sekunden>`

   Der Standardwert ist 120 Sekunden.

   Beispiel: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. Erstellen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*, um Informationen über Patches für Drittanbieter-Programme abzurufen, die auf den verwalteten Geräten installiert sind, und legen Sie anschließend den Aufgabenzeitplan fest.

7. Erstellen Sie die Aufgabe *Schwachstellen schließen*, um Patches anzugeben, die zum Schließen von Schwachstellen in Drittanbieter-Programmen verwendet werden, und legen Sie anschließend den Aufgabenzeitplan fest.

   Starten Sie die Aufgaben manuell, wenn Sie diese früher ausführen möchten, als im Zeitplan angegeben. Die Ausführungsreihenfolge der Aufgaben ist wichtig. Die Aufgabe *Schwachstellen schließen* muss nach der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* ausgeführt werden.

8. Starten Sie den Administrationsserver-Dienst neu.

Der Administrationsserver mit Internetzugang ist bereit, Updates herunterzuladen und an isolierte Administrationsserver zu übertragen. Bevor Sie mit dem Schließen von Schwachstellen beginnen, müssen Sie die isolierten Administrationsserver konfigurieren.

Konfigurieren von isolierten Administrationsservern, Schwachstellen in einem isolierten Netzwerk zu schließen

Bereiten Sie nach der Konfiguration des Administrationsservers mit Internetzugang alle isolierten Administrationsserver in Ihrem Netzwerk vor, um auf den verwalteten Geräten, die mit isolierten Administrationsservern verbunden sind, Schwachstellen zu schließen und Updates zu installieren.

Um isolierte Administrationsserver zu konfigurieren, führen Sie für jeden Administrationsserver die folgenden Schritte aus:

1. Aktivieren Sie einen Lizenzschlüssel für die Funktion "Schwachstellen- und Patch-Management" (VAPM).
2. Erstellen Sie zwei Ordner auf der Festplatte, auf welcher der Administrationsserver installiert ist:
   - Ordner für die Liste mit erforderlichen Updates
   - Ordner für Patches

   Sie können diesen Ordnern beliebige Namen geben.
3. Weisen Sie der Gruppe "KLAdmins" für die erstellten Ordner die Berechtigung **Ändern** zu. Verwenden Sie dazu die Standardverwaltungstools des Betriebssystems.
4. Verwenden Sie das Dienstprogramm "klscflag", um die Pfade zu diesen Ordnern in den Eigenschaften des Administrationsservers anzugeben.

   Öffnen Sie die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".
5. Führen Sie in der Befehlszeile die folgenden Befehle aus:
   - Um den Pfad zum Patch-Ordner festzulegen:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<Pfad zum Ordner>"`
   - So legen Sie den Pfad zum Ordner für die Liste mit erforderlichen Updates fest:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<Pfad zum Ordner>"`

   Beispiel: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "/FolderForPatches"`
6. Verwenden Sie bei Bedarf das Tool "klscflag", um anzugeben, wie oft der isolierte Administrationsserver nach neuen Patches suchen soll:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <Wert in Sekunden>`

   Standardmäßig ist der Wert auf 120 Sekunden eingestellt.

   Beispiel: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 120`
7. Verwenden Sie bei Bedarf das Tool "klscflag", um die SHA256-Hashes der Patches zu berechnen:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   Durch Ausführen dieses Befehls stellen Sie sicher, dass die Patches während der Übertragung auf den isolierten Administrationsserver nicht verändert wurden und dass Sie die richtigen Patches mit den erforderlichen Updates erhalten haben.

Standardmäßig berechnet Kaspersky Security Center Linux keine SHA256-Hashes für Patches. Nachdem der isolierte Administrationsserver die Patches erhalten hat, berechnet Kaspersky Security Center Linux bei aktivierter Option die Hashes und vergleicht die berechneten Werte mit den Hashes, die in der Administrationsserver-Datenbank gespeichert sind. Wenn der berechnete Hash nicht mit dem Hash in der Datenbank übereinstimmt, wird ein Fehler gemeldet und Sie müssen den inkorrekten Patch ersetzen.

8. Erstellen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*, um Informationen über Patches für Drittanbieter-Programme abzurufen, die auf den verwalteten Geräten installiert sind, und legen Sie anschließend den Aufgabenzeitplan fest.

9. Erstellen Sie die Aufgabe *Schwachstellen schließen*, um Patches anzugeben, die zum Schließen von Schwachstellen in Drittanbieter-Programmen verwendet werden, und legen Sie anschließend den Aufgabenzeitplan fest.

   Starten Sie die Aufgaben manuell, wenn Sie diese früher ausführen möchten, als im Zeitplan angegeben. Die Ausführungsreihenfolge der Aufgaben ist wichtig. Die Aufgabe *Schwachstellen schließen* muss nach der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* ausgeführt werden.

10. Starten Sie den Administrationsserver-Dienst neu.

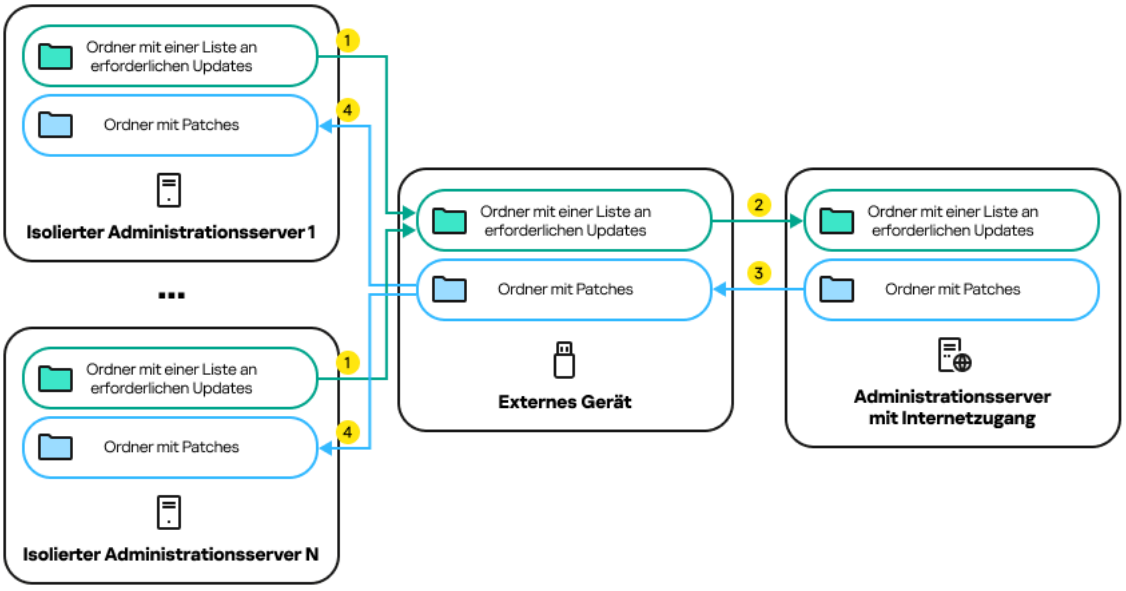
Nachdem Sie alle Administrationsserver konfiguriert haben, können Sie die Patches und die Liste mit erforderlichen Updates übertragen und die Schwachstellen in Drittanbieter-Programmen auf den verwalteten Geräten innerhalb des isolierten Netzwerks beheben.

Übertragen von Patches und Installieren von Updates in einem isolierten Netzwerk

Nachdem Sie die Konfiguration der Administrationsserver abgeschlossen haben, können Sie Patches mit erforderlichen Updates vom Administrationsserver mit Internetzugang auf isolierte Administrationsserver übertragen. Sie können Updates beliebig oft übertragen und installieren, z. B. einmal oder mehrmals täglich.

Sie benötigen ein externes Gerät, beispielsweise einen Wechseldatenträger, um Patches und die Liste der erforderlichen Updates zwischen den Administrationsservern zu übertragen. Stellen Sie daher sicher, dass das externe Gerät über genügend Speicherplatz zum Herunterladen und Speichern der Patches verfügt.

Der Vorgang zur Übertragung von Patches und der Liste mit erforderlichen Updates ist in der folgenden Abbildung dargestellt:



Vorgang zur Übertragung von Patches und der Liste mit erforderlichen Updates zwischen dem Administrationsserver mit Internetzugang und den isolierten Administrationsservern

So installieren Sie Updates und schließen Schwachstellen auf verwalteten Geräten, die mit isolierten Administrationsservern verbunden sind:

1. Starten Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen*, wenn diese noch nicht ausgeführt wird.

2. Verbinden Sie ein externes Gerät mit einem der isolierten Administrationsserver.

3. Erstellen Sie zwei Ordner auf dem externen Gerät: einen für die Liste mit erforderlichen Updates und einen für Patches. Sie können diesen Ordnern beliebige Namen geben.

   Falls Sie diese Ordner bereits erstellt haben, bereinigen Sie diese.

4. Kopieren Sie die Liste der erforderlichen Updates von jedem isolierten Administrationsserver und fügen Sie diese Liste auf dem externen Gerät in den Ordner für die Liste mit erforderlichen Updates ein.

   Dadurch führen Sie alle Listen, die von den einzelnen isolierten Administrationsservern erfasst wurden, in einem Ordner zusammen. Dieser Ordner enthält Binärdateien mit den IDs von Patches, die für alle isolierten Administrationsserver erforderlich sind.

5. Verbinden Sie das externe Gerät mit dem Administrationsserver, der Internetzugang hat.

6. Kopieren Sie die Liste mit erforderlichen Updates vom externen Gerät und fügen Sie diese Liste auf dem Administrationsserver mit Internetzugang in den Ordner für die Liste mit erforderlichen Updates ein.

   Auf dem Administrationsserver werden automatisch alle erforderlichen Patches aus dem Internet in den Ordner für Patches heruntergeladen. Dies kann mehrere Stunden dauern.

7. Überprüfen Sie, ob alle erforderlichen Patches heruntergeladen wurden. Gehen Sie dazu wie folgt vor:

   - Überprüfen Sie den Ordner für Patches auf dem Administrationsserver mit Internetzugang. Alle Patches, die in der Liste mit erforderlichen Updates angegeben sind, sollten in den erforderlichen Ordner heruntergeladen werden. Dies ist praktischer, wenn eine kleine Anzahl von Patches benötigt wird.

   - Erstellen Sie ein spezielles Skript (z. B. ein Shell-Skript). Wenn Sie eine hohe Anzahl von Patches erhalten, ist es schwierig, selbst zu überprüfen, ob alle Patches heruntergeladen wurden. In solchen Fällen ist es ratsam, die Überprüfung zu automatisieren.

8. Kopieren Sie die Patches vom Administrationsserver mit Internetzugang und fügen Sie die Patches in den entsprechenden Ordner auf Ihrem externen Gerät ein.

9. Übertragen Sie die Patches auf jeden der isolierten Administrationsserver. Legen Sie die Patches in einem dafür vorgesehenen Ordner ab.

Als Ergebnis erstellt jeder isolierte Administrationsserver eine aktuelle Liste mit Updates, die für jene verwalteten Geräte erforderlich sind, die mit dem aktuellen Server verbunden sind. Nachdem der Administrationsserver mit Internetzugang die Liste mit erforderlichen Updates erhalten hat, lädt der Administrationsserver die Patches aus dem Internet herunter. Wenn diese Patches auf isolierte Administrationsservern verfügbar werden, verarbeitet die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* die Patches. Auf diese Weise werden Updates auf verwalteten Geräten installiert und Schwachstellen in Drittanbieter-Programmen behoben.

Während die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* ausgeführt wird, darf das Gerät des Administrationsservers nicht neu gestartet werden und die Aufgabe *Backup der Daten des Administrationsservers anlegen* nicht ausgeführt werden (sie führt ebenfalls zum Neustart). Dadurch wird die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* unterbrochen und die Updates werden nicht installiert. In diesem Fall müssen Sie diese Aufgabe manuell neu starten oder warten, bis die Aufgabe nach dem festgelegten Zeitplan gestartet wird.

Übertragung von Patches und Installation von Updates in einem isolierten Netzwerk deaktivieren

Sie können die Übertragung von Patches an isolierte Administrationsserver deaktivieren. Dies kann nützlich sein, wenn Sie einen oder mehrere Administrationsserver aus dem isolierten Netzwerk herausnehmen möchten. Dadurch können Sie die Anzahl der Patches und die Download-Dauer reduzieren.

So deaktivieren Sie die Übertragung von Patches an isolierte Administrationsserver:

1. Wenn Sie alle Administrationsserver aus der Isolation entfernen möchten, löschen Sie in den Eigenschaften des Administrationsservers mit Internetzugang die Pfade zu den vorgesehenen Ordnern für die Patches sowie für die Liste der erforderlichen Updates. Wenn Sie bestimmte Administrationsserver im isolierten Netzwerk behalten möchten, überspringen Sie diesen Schritt.

   Öffnen Sie die Befehlszeile und wechseln Sie anschließend in das Verzeichnis mit dem Tool "klscflag". Das Tool "klscflag" befindet sich in dem Verzeichnis, in dem der Administrationsserver installiert ist. Der Standardinstallationspfad lautet "/opt/kaspersky/ksc64/sbin".

   Führen Sie in der Befehlszeile die folgenden Befehle aus:

   - So löschen Sie den Pfad des Ordners für Patches:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```

- So löschen Sie den Pfad des Ordners für die Liste mit erforderlichen Updates:
  `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""`

2. Wenn Sie die Pfade zu den Ordnern gelöscht haben, starten Sie den Dienst auf dem Administrationsserver mit Internetzugang neu.

3. Löschen Sie in den Eigenschaften jedes isolierten Administrationsservers, den Sie aus dem isolierten Netzwerk entfernen möchten, die Pfade der Ordner für Patches und für die Liste der erforderlichen Updates.

   Führen Sie in der Befehlszeile die folgenden Befehle unter einem Benutzerkonto mit Root-Rechten aus:

   - Um den Pfad des Ordners für Patches zu löschen:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""`

   - So löschen Sie den Pfad des Ordners für die Liste mit erforderlichen Updates:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""`

4. Starten Sie den Dienst auf jedem Administrationsserver neu, auf dem Sie die Pfade zu den Ordnern gelöscht haben.

Wenn Sie den Administrationsserver mit Internetzugang neu konfiguriert haben, werden über Kaspersky Security Center Linux keine Patches mehr übertragen.

Wenn Sie nur bestimmte Administrationsserver neu konfiguriert und aus dem isolierten Netzwerk entfernt haben, erhalten diese keine Patches mehr über Kaspersky Security Center Linux. Nur die Administrationsserver, die im isolierten Netzwerk verbleiben, erhalten weiterhin Patches.

Wenn Sie die Behebung von Schwachstellen auf deaktivierten isolierten Administrationsservern später starten möchten, müssen Sie diese Administrationsserver und den Administrationsserver mit Internetzugang neu konfigurieren.

API-Referenzhandbuch

Dieses Kaspersky Security Center OpenAPI-Referenzhandbuch soll Sie bei den folgenden Aufgaben unterstützen:

- Automatisierung und Individualisierung. Sie können dadurch Aufgaben automatisieren, die nicht manuell ausgeführt werden sollen. Beispielsweise können Sie Kaspersky Security Center OpenAPI dazu verwenden, Scripte zu erstellen und auszuführen, die das Entwickeln und Pflegen einer Struktur von Administrationsgruppen vereinfachen.

- Individuelle Entwicklung. Mit OpenAPI können Sie eine Client-Anwendung entwickeln.

Sie können das Suchfeld auf der rechten Seite des Bildschirms verwenden, um im OpenAPI-Referenzhandbuch die von Ihnen benötigten Informationen zu finden.

OPENAPI-REFERENZHANDBUCH

Skriptbeispiele

Das OpenAPI-Referenzhandbuch enthält Beispiele für die in der folgenden Tabelle aufgeführten Python-Skripts. Diese Beispiele zeigen, wie Sie OpenAPI-Methoden aufrufen und verschiedene Aufgaben zum Schutz Ihres Netzwerks automatisch ausführen können, z. B. das Erstellen einer "primär/sekundär"-Hierarchie, das Ausführen von Aufgaben in Kaspersky Security Center Linux oder das Zuweisen von Verteilungspunkten. Sie können die Beispiele unverändert ausführen oder Ihre eigenen Skripts basierend auf den Beispielen erstellen.

Um die OpenAPI-Methoden aufzurufen und Skripte auszuführen:

Installieren Sie das Paket KlAkOAPI aus dem Archiv "KlAkOAPI.tar.gz" auf einem Gerät mit installiertem Administrationsserver.

Das KlAkOAPI-Paket enthält eine Reihe von Beispielen, die typische Vorgänge ausführen. Das Aufrufen der OpenAPI-Methoden und das Ausführen von Beispielen und eigenen Skripten ist nur auf Geräten möglich, auf denen der Administrationsserver und das KlAkOAPI -Paket installiert sind. Das Archiv "KlAkOAPI.tar.gz" mit dem Paket befindet sich im Installationsordner von Kaspersky Security Center Linux.

Benutzerszenarien und Beispiele für entsprechende Kaspersky Security Center OpenAPI-Methoden

Beispiel	Ziel des Beispiels	Szenario
Loggen von KlAkParams	Unter Verwendung der `KlAkParams` -Datenstruktur können Sie Daten extrahieren und verarbeiten. Das ist ein Beispiel für die Arbeit mit dieser Datenstruktur. Die Ausgabe des Beispiels kann auf verschiedene Weisen präsentiert werden. Sie können die Daten erhalten, um eine HTTP-Methode zu versenden, oder um Sie in Ihrem Code zu verwenden.	Überwachung und Berichterstattung
"Primär/Sekundär"-Hierarchie erstellen und löschen	Sie können einen sekundären Administrationsserver hinzufügen und so eine Hierarchie vom Typ "primär/sekundär" festlegen. Alternativ können Sie den sekundären Administrationsserver von der Hierarchie trennen.	Erstellen einer Hierarchie von Administrationsservern, Hinzufügen eines sekundären Administrationsservers und Löschen einer Hierarchie von Administrationsservern
Netzwerklisten-Dateien mittels Verbindungs-Gateway auf den angegebenen Host herunterladen	Unter Verwendung eines Verbindungs-Gateways können Sie sich mit dem Administrationsagenten des benötigten Geräts verbinden und anschließend die Datei mit der Netzwerkliste auf Ihr Gerät herunterladen.	Verteilungspunkte und Verbindungs-Gateways anpassen

Beispiel	Ziel des Beispiels	Szenario
Einen Lizenzschlüssel, der sich in der Datenverwaltung des primären Administrationsservers befindet, auf sekundären Administrationsservern installieren	Sie können sich mit dem primären Administrationsserver verbinden, von ihm einen erforderlichen Lizenzschlüssel herunterladen, und diesen Schlüssel an alle in der Hierarchie enthaltenen sekundären Administrationsserver weiterleiten.	Lizenzierung der verwalteten Anwendungen
Erstellen eines Berichts über gültige Benutzerberechtigungen	Sie können verschiedene Berichte erstellen. Unter anderem können Sie den Bericht über gültige Benutzerberechtigungen unter Verwendung dieses Beispiels erstellen. Dieser Bericht gibt die Berechtigungen eines Benutzers in Abhängigkeit seiner oder ihrer Gruppe und Rolle an. Sie können den Bericht in den folgenden Formaten herunterladen: HTML, PDF oder Excel.	Bericht erstellen und anzeigen
Starten der Aufgabe für ein Gerät	Unter Verwendung eines Verbindungs-Gateways können Sie sich mit dem Administrationsagenten des benötigten Geräts verbinden und anschließend die notwendige Aufgabe starten.	Aufgaben manuell starten
Registrieren von Verteilungspunkten für Geräte in einer Gruppe	Sie können verwalteten Geräten die Rolle eines Verteilungspunkts (früher bekannt als "Update-Agent") zuweisen.	Datenbanken und Anwendungen von Kaspersky aktualisieren
Alle Gruppen durchzählen	Sie können mit Administrationsgruppen verschiedene Aktionen ausführen. Das Beispiel zeigt Folgendes: • Eine ID der Root-Gruppe der "Verwalteten Geräte" abrufen • Durch die Gruppenhierarchie bewegen • Die vollständige, erweiterte Gruppenhierarchie, einschließlich ihrer Namen und Vierschachtelungen abrufen	Administrationsserver konfigurieren
Aufgaben durchzählen, Aufgabenstatistiken abfragen und Aufgaben ausführen	Die folgenden Informationen können Sie abfragen: • Verlauf des Aufgabenprozesses • Aktueller Aufgabenstatus • Anzahl der Aufgaben mir unterschiedlichen Statuswerten Sie können auch eine Aufgabe starten. Standardmäßig startet das Beispiel eine Aufgabe, nachdem es Statistiken ausgegeben hat.	Aufgaben verwalten
Eine Aufgabe erstellen und ausführen	Sie können eine Aufgabe erstellen. Geben Sie in dem Beispiel die folgenden Aufgabenparameter an: • Typ • Art der Ausführung • Name • Gerätegruppe, auf welche die Aufgabe angewendet wird Standardmäßig erstellt das Beispiel eine Aufgabe des Typs "Nachricht anzeigen". Sie können diese Aufgabe für alle verwalteten Geräte des Administrationsservers ausführen. Bei Bedarf können Sie eigene Aufgabenparameter angeben.	Aufgaben erstellen
Lizenzschlüssel durchzählen	Sie können eine Liste mit allen aktiven Lizenzschlüsseln für Kaspersky-Anwendungen abrufen, die auf den verwalteten Geräten des Administrationsservers installiert sind. Die Liste enthält detaillierte Informationen über jeden Lizenzschlüssel, darunter Name, Typ oder Ablaufdatum.	Informationen zu verwendeten Lizenzschlüsseln anzeigen
Einen internen Benutzer erstellen und auffinden	Sie können ein Benutzerkonto zur weiteren Bearbeitung erstellen.	Benutzerkonto für einen internen Benutzer hinzufügen
Eine benutzerdefinierte Kategorie erstellen	Sie können eine Programmkategorie mit den benötigten Parametern erstellen.	Manuell zu erweiternde Programmkategorie erstellen

Beispiel	Ziel des Beispiels	Szenario
Benutzer mittels SrvView durchzählen	Sie können die Klasse SrvView verwenden, um detaillierte Informationen vom Administrationsserver abzufragen. Unter Verwendung dieses Beispiels können Sie unter anderem eine Liste der Benutzer abrufen.	Benutzer und Benutzerrollen verwalten
Interne Benutzer erstellen, Android-Installationspaket erstellen und per E-Mail versenden	Sie können interne Benutzer mithilfe der Klasse SecurityPolicy erstellen sowie ein Android-Installationspaket erstellen und es per E-Mail an die Benutzer senden.	Hinzufügen eines Benutzerkontos eines internen Benutzers

Anwendungen, die über OpenAPI mit Kaspersky Security Center Linux interagieren

Einige Anwendungen können über OpenAPI mit Kaspersky Security Center Linux interagieren. Zu solchen Anwendungen gehören beispielsweise Kaspersky Anti Targeted Attack Platform und Kaspersky Security for Virtualization. Dies kann auch ein von Ihnen entwickelte benutzerdefinierte Client-Anwendung auf Basis von OpenAPI sein.

Anwendungen, die über OpenAPI mit Kaspersky Security Center Linux interagieren, verbinden sich mit dem Administrationsserver. Wenn Sie für die Verbindung mit dem Administrationsserver eine Allow-Liste mit IP-Adressen konfiguriert haben, fügen Sie die IP-Adressen von den Geräten hinzu, auf denen Anwendungen laufen, welche die Kaspersky Security Center Linux-OpenAPI verwenden. Weitere Informationen darüber, ob die von Ihnen verwendete Anwendung durch OpenAPI unterstützt wird, entnehmen Sie der Hilfe der entsprechenden Anwendung.

Bewährte Verfahren für Dienstanbieter

Dieser Abschnitt enthält Informationen zur Konfiguration und Verwendung von Kaspersky Security Center Linux.

Dieser Abschnitt enthält Empfehlungen für die Bereitstellung, Einstellungen und Nutzung des Programms, sowie Möglichkeiten zur Lösung von typischen Problemen, die bei der Ausführung des Programms entstehen.

Bereitstellung von Kaspersky Security Center Linux planen

Bei der Planung der Verteilung der Komponenten von Kaspersky Security Center Linux im Unternehmensnetzwerk müssen die folgenden Faktoren beachtet werden:

- Gesamtzahl der Geräte
- Anzahl der MSP-Kunden

Ein Administrationsserver kann nicht mehr als 50.000 Geräte verwalten. Wenn die Gesamtzahl der Geräte im Unternehmensnetzwerk 50.000 überschreitet, müssen von Seiten des Anbieters mehrere Administrationsserver verteilt werden, die zur einfacheren zentralen Verwaltung in einer Hierarchie zusammengefasst sind.

Auf einem einzigen Administrationsserver können bis zu 500 virtuelle Server erstellt werden, was bedeutet, dass pro 500 MSP-Kunden ein separater Administrationsserver benötigt wird.

Bei der Planung der Bereitstellung muss die Notwendigkeit zur Angabe des speziellen X.509-Zertifikats für den Administrationsserver in Betracht gezogen werden. Die Zuweisung des X.509-Zertifikates für den Administrationsserver kann in folgenden Fällen (unvollständige Liste) hilfreich sein:

- Zur Untersuchung des SSL-Datenverkehrs (Secure Socket Layer) über SSL Termination Proxy
- Zur Angabe der gewünschten Werte für die Felder des Zertifikats
- Zur Gewährleistung der erwünschten Verschlüsselungsstärke des Zertifikats

Internetzugriff für den Administrationsserver bereitstellen

Damit die Geräte, die sich im Netzwerk des Kunden befinden, über das Internet mit dem Administrationsserver interagieren können, müssen die folgenden Ports des Administrationsservers verfügbar sein:

- 13000 TCP – TLS-Port des Administrationsservers zur Verbindung der im Kundennetzwerk bereitgestellten Administrationsagenten
- 8061 TCP – HTTPS-Port für die Veröffentlichung von autonomen Paketen über die Kaspersky Security Center Web Console
- 8060 TCP – HTTP-Port für die Veröffentlichung von autonomen Paketen über die Kaspersky Security Center Web Console

- 13292 TCP – TLS-Port, der lediglich für die Verwaltung mobiler Geräte erforderlich ist
- 8080 TCP – HTTPS-Port der Kaspersky Security Center Web Console

Typische Konfiguration von Kaspersky Security Center Linux

Auf den MSP-Servern sind ein oder mehrere Administrationsserver vorhanden. Die Anzahl der Administrationsserver kann sowohl ausgehend von der vorhandenen verfügbaren Hardware als auch in Abhängigkeit von der Gesamtmenge der verwalteten MSP-Kunden oder der Gesamtmenge der verwalteten Geräte ausgewählt werden.

Ein Administrationsserver kann bis zu 50.000 Geräte verwalten. Die Möglichkeit einer Erhöhung der Anzahl der verwalteten Geräte in nächster Zukunft muss berücksichtigt werden: es kann sich als wünschenswert erweisen, eine etwas kleinere Anzahl von Geräten mit einem Administrationsserver zu verbinden.

Auf einem einzigen Administrationsserver können bis zu 500 virtuelle Server erstellt werden, was bedeutet, dass pro 500 MSP-Kunden ein separater Administrationsserver benötigt wird.

Wenn es mehrere Server gibt, ist es empfehlenswert, sie in einer Hierarchie zusammenzufassen. Das Verwenden einer Hierarchie der Administrationsserver erlaubt Ihnen, das Duplizieren von Richtlinien und Aufgaben zu vermeiden und mit allen verwalteten Geräte zu arbeiten, als ob sie von einem Administrationsserver verwaltet würden: Geräte suchen, Geräteauswahlen erstellen, Berichte erstellen.

Auf jedem virtuellen Server, der dem MSP-Kunden entspricht, müssen ein oder mehrere Verteilungspunkte bestimmt werden. Wenn die Verbindung zwischen den MSP-Kunden und dem Administrationsserver über das Internet hergestellt wird, kann es sinnvoll sein, für die Verteilungspunkte die *Aufgabe zum Download von Updates in die Datenverwaltung von Verteilungspunkten* zu erstellen, damit die Verteilungspunkte die Updates nicht vom Administrationsserver, sondern direkt von den Kaspersky-Servern herunterladen.

Wenn ein Teil der Geräte im Netzwerk des MSP-Kunden keinen direkten Internetzugang besitzt, müssen die Verteilungspunkte in den Gateway-Modus (Connection Gateway) versetzt werden. In diesem Fall werden die Administrationsagenten auf den Geräten im Netzwerk des MSP-Kunden (zwecks Synchronisierung) nicht direkt, sondern über ein Gateway mit dem Administrationsserver verbunden.

Da der Administrationsserver das Netzwerk des MSP-Kunden aller Wahrscheinlichkeit nach nicht abfragen kann, ist es sinnvoll, das Ausführen dieser Funktion auf einen der Verteilungspunkte zu übertragen.

Der Administrationsserver kann an verwaltete Geräte, die sich im Netzwerk des MSP-Kunden hinter NAT befinden, keine Benachrichtigungen an den Port 15000 UDP senden. Für die Behebung dieses Problems ist es sinnvoll, in den Eigenschaften der Geräte, die als Verteilungspunkte dienen und die im Gateway-Modus ausgeführt werden (Connection Gateway), den Modus zur ständigen Verbindung mit dem Administrationsserver (Option **Verbindung mit Administrationsserver nicht trennen**) zu aktivieren. Der Modus der ständigen Verbindung ist verfügbar, wenn die Gesamtanzahl der Verteilungspunkte 300 nicht überschreitet.

Ein MSP-Kunde möchte unter Umständen die Android- und iOS-Geräte der Mitarbeiter verwalten. Der Administrationsserver verwaltet mobile Geräte über TLS mittels TCP-Port 13292.

Über Verteilungspunkte

Ein Gerät mit Administrationsagent kann als Verteilungspunkt verwendet werden. In diesem Modus kann der Administrationsagent folgende Tätigkeiten ausführen:

- Dateien an Client-Geräte übertragen, einschließlich:
  - Updates für die Datenbanken und Programm-Module von Kaspersky

    Die Updates können sowohl vom Administrationsserver als auch von den Kaspersky-Servern abgerufen werden. Im zweiten Fall muss für das Gerät, das als Verteilungspunkt dient, die Aufgabe *Download von Updates in die Datenverwaltung der Verteilungspunkte* erstellt werden.
  - Updates für Drittanbieter-Programme
  - Installationspakete
- Software auf anderen Geräten installieren, einschließlich Ausführung der erstmaligen Bereitstellung der Administrationsagenten auf den Geräten.
- Das Netzwerk abfragen, um neue Geräte und aktualisierte Informationen über die bereits bekannten Geräte zu finden. Der Verteilungspunkt kann dieselben Methoden zur Gerätesuche ausführen wie der Administrationsserver.

Die Bereitstellung von Verteilungspunkten im Unternehmensnetzwerk verfolgt die folgenden Ziele:

- Reduzierung der Auslastung des Administrationsservers in dem Fall, dass der Administrationsserver als Update-Quelle dient.
- Optimierung des Internet-Datenverkehrs, da sich in diesem Fall nicht jedes Gerät im Netzwerk des MSP-Kunden an die Server von Kaspersky oder an den Administrationsserver wenden muss, um Updates zu erhalten.
- Wenn dem Administrationsserver der Zugriff auf die Geräte hinter der NAT (vom Standpunkt des Administrationsservers aus) des Netzwerks des MSP-Kunden gewährt wird, kann der Administrationsserver folgende Aktionen durchführen:
  - Nachrichten an Geräte in IPv4- oder IPv6-Netzwerken über UDP versenden
  - Das IPv4- oder IPv6-Netzwerk abfragen
  - Erstmalige Bereitstellung ausführen
  - Als Push-Server fungieren

Ein Verteilungspunkt wird für eine Administrationsgruppe bestimmt. In diesem Fall umfasst der Gültigkeitsbereich für den Verteilungspunkt alle Geräte, die sich in einer solcher Administrationsgruppe und allen ihren Untergruppen befinden. Dabei muss sich das Gerät, das als Verteilungspunkt fungiert, nicht in der Administrationsgruppe befinden, für die es bestimmt wurde.

Sie können einen Verteilungspunkt als Verbindungs-Gateway nutzen. Die Geräte, die sich in diesem Verteilungspunkt befinden, werden in diesem Fall nicht direkt, sondern durch ein Gateway mit dem Administrationsserver verbunden. Der vorliegende Modus ist in Szenarien nützlich, bei denen zwischen den Geräten mit dem Administrationsagenten und dem Administrationsserver keine direkte Verbindung möglich ist.

Geräte, die als Verteilungspunkte fungieren, müssen vor unberechtigtem Zugriff (auch physischer Natur) geschützt werden.

Hierarchie des Administrationsservers

Einige Kundenunternehmen wie MSPs betreiben möglicherweise mehrere Administrationsserver. Die Verwaltung mehrerer vereinzelter Administrationsserver ist unpraktisch, deshalb es ist zweckmäßig, sie in einer Hierarchie zusammenzufassen. In einer Hierarchie kann ein Linux-basierter Administrationsserver sowohl als primärer Server als auch als sekundärer Server fungieren. Der primäre Linux-basierte Server kann sowohl Linux-basierte als auch Windows-basierte sekundäre Server verwalten. Ein primärer Server auf Windows-Basis kann einen sekundären Server auf Linux-Basis verwalten.

Eine "Primär/Sekundär"-Konfiguration für zwei Administrationsserver bietet die folgenden Möglichkeiten:

- Der sekundäre Administrationsserver erbt vom primären Administrationsserver die Richtlinien Aufgaben, Benutzerrollen und Installationspakete, wobei duplizierte Einstellungen entfernt werden.
- Die Geräteauswahlen auf dem primären Administrationsserver können Geräte der sekundären Administrationsserver einschließen.
- Die Berichte auf dem primären Administrationsserver können Daten (einschließlich ausführlicher Informationen) der sekundären Administrationsserver einschließen.
- Als Update-Quelle für einen sekundären Administrationsserver kann ein primärer Administrationsserver verwendet werden.

Der primäre Administrationsserver empfängt Daten von sekundären, nicht-virtuellen Administrationsservern nur im Rahmen der oben aufgeführten Optionen. Diese Einschränkung gilt nicht für virtuelle Administrationsserver, welche die Datenbank mit ihrem primären Administrationsserver teilen.

Die Hierarchie der Administrationsserver unterstützt den Mandantenfähigkeitsmodus. Dieser Modus ermöglicht es einem Hauptadministrator, mehrere Clients unabhängig voneinander zentral zu verwalten. Jedes Kundenunternehmen oder Büro ist von anderen isoliert und wird als Mandant bezeichnet. Sie können einem Mandanten mehrere verwaltete Geräte mit den dazugehörigen Daten, Einstellungen, Richtlinien und Aufgaben zuweisen und die Benutzerrechte nach Mandanten konfigurieren.

Ein primärer Administrationsserver, der in der Hauptinfrastruktur des Unternehmens installiert ist, fungiert als primärer Mandant. Der primäre Administrationsserver ermöglicht es sekundären oder virtuellen Administrationsservern – seinen isolierten Mandanten –, selbstständig ihre eigenen Ereignisse zu empfangen und zu verarbeiten und mit ihren eigenen Ressourcen, Diensten und Konfigurationen zu arbeiten.

Ein Dienstanbieter mit mehreren Kundenunternehmen kann die Funktionalität von Kaspersky Security Center Linux einschließlich der Aggregation von Alarmen und Reaktionsmaßnahmen für jedes Kundenunternehmen unabhängig voneinander bereitstellen. Zu diesem Zweck verbindet der Dienstanbieter sekundäre oder virtuelle Administrationsserver als Mandanten für jedes Kundenunternehmen. Der Dienstanbieter stellt Dienste unter Verwendung seines eigenen Personals und seiner eigenen Ressourcen bereit.

Virtuelle Administrationsserver

Im Rahmen des physischen Administrationsservers können mehrere virtuelle Administrationsserver erstellt werden, die in vieler Hinsicht sekundären Servern ähnlich sind. Im Vergleich zum Modell des geteilten Zugriffs, der auf den Listen der Zugriffskontrolle (ACL) beruht, ist das Modell der virtuellen Administrationsserver funktioneller und bietet eine hohe Stufe der Isolierung. Neben der eigenen Struktur der Administrationsgruppen für verwaltete Geräte mit Richtlinien und Aufgaben hat jeder virtuelle Administrationsserver auch eine eigene Gruppe von nicht zugeordneten Geräten, die über eigene Sätze von Berichten, Geräteauswahlen und Ereignissen, Installationspakete, Regeln zur Verschiebung von Geräten usw. verfügt. Um MSP-Kunden bestmöglich voneinander zu isolieren, wird empfohlen, die Funktionalität virtueller Administrationsserver zu verwenden. Außerdem ermöglicht das Erstellen eines virtuellen Administrationsservers für jeden MSP-Kunden, den Kunden grundlegende Möglichkeiten zur Verwaltung des eigenen Netzwerkes mittels Kaspersky Security Center Web Console zu gewähren.

Virtuelle Administrationsserver ähneln in vieler Hinsicht sekundären Administrationsservern, haben jedoch die folgenden Unterschiede:

- Einem virtuellen Administrationsserver fehlt eine Vielzahl der globalen Einstellungen und eigenen TCP-Ports
- Ein virtueller Administrationsserver hat keine sekundären Administrationsserver
- Ein virtueller Administrationsserver kann keine eigenen virtuellen Administrationsserver haben
- Auf dem physischen Administrationsserver sind die Geräte, Gruppen, Ereignisse und Objekte der verwalteten Geräte (Elemente der Quarantäne, Programm-Registry und andere) aller seiner virtuellen Administrationsserver sichtbar
- Ein virtueller Administrationsserver kann das Netzwerk nur mittels der mit ihm verbundenen Verteilungspunkte abfragen

Bereitstellung und Erstkonfiguration

Kaspersky Security Center Linux ist ein verteiltes Programm. Im Lieferumfang von Kaspersky Security Center Linux sind folgende Komponenten enthalten:

- Administrationsserver – die zentrale Komponente, die für die Verwaltung der Geräte des Unternehmens und für die Datenspeicherung im DBMS verantwortlich ist.
- Kaspersky Security Center Web Console — Webschnittstelle zum Administrationsserver für die Ausführung grundlegender Vorgänge. Sie können diese Komponente auf jedem Gerät installieren, das die Hard- und Softwarevoraussetzungen erfüllt.
- Administrationsagent – dient zur Verwaltung der auf einem Gerät installierten Sicherheitsanwendungen sowie zum Empfangen von Informationen über dieses Gerät. Die Administrationsagenten werden auf den Geräten des Unternehmens installiert.

Die Bereitstellung von Kaspersky Security Center Linux im Unternehmensnetzwerk verläuft auf folgende Weise:

- Installation des Administrationsservers
- Installation der Kaspersky Security Center Web Console
- Installation des Administrationsagenten und der Sicherheitsanwendung auf den Geräten des Unternehmens

Installationsempfehlungen für den Administrationsserver

Dieser Abschnitt enthält Empfehlungen in Bezug auf die Installation des Administrationsservers. Im Abschnitt finden Sie ferner Szenarien für die Nutzung des freigegebenen Ordners auf dem Gerät mit dem Administrationsserver zur Bereitstellung des Administrationsagenten auf den Client-Geräten.

Benutzerkonten für die Dienste des Administrationsservers auf dem Failover-Cluster erstellen

Bevor Sie mit der Bereitstellung von Kaspersky Security Center Linux auf einem Failover-Cluster beginnen, müssen Sie Konten für die Dienste von Kaspersky Security Center Linux erstellen.

Führen Sie dazu die folgenden Schritte auf dem aktiven Knoten, dem passiven Knoten und dem Dateiserver aus:

1. Erstellen Sie eine Gruppe mit dem Namen "kladmins" und weisen Sie allen drei Gruppen dieselbe GID zu.
2. Erstellen Sie ein Benutzerkonto mit dem Namen "ksc" und weisen Sie allen drei Benutzerkonten dieselbe UID zu. Legen Sie für die erstellten Konten die primäre Gruppe "kladmins" fest.
3. Erstellen Sie ein Benutzerkonto mit dem Namen "rightless" und weisen Sie allen drei Benutzerkonten dieselbe UID zu. Legen Sie für die erstellten Konten die primäre Gruppe "kladmins" fest.

Auswahl des DBMS

In der nachfolgenden Tabelle sind die zulässigen DBMS-Varianten und deren Empfehlungen und Einschränkungen zur Verwendung aufgeführt.

Empfehlungen und Einschränkungen der DBMSs

DBMS	Empfehlungen und Einschränkungen
MySQL (siehe unterstützte Versionen)	Verwenden Sie dieses DBMS, wenn Sie einen Administrationsserver für bis zu 20.000 Geräte verwenden möchten.
MariaDB (siehe unterstützte Versionen)	Verwenden Sie dieses DBMS, wenn Sie einen Administrationsserver für bis zu 20.000 Geräte verwenden möchten.

PostgreSQL, Postgres Pro (siehe unterstützte Versionen)	Verwenden Sie dieses DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 50.000 Geräte einzusetzen.
Tantor (siehe unterstützte Versionen)	Verwenden Sie dieses DBMS, wenn Sie beabsichtigen, einen einzelnen Administrationsserver für bis zu 50.000 Geräte einzusetzen. Das Tantor-DBMS wird nur von Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.8) unterstützt.

Informationen zur Installation des ausgewählten DBMS finden Sie in der DBMS-Dokumentation.

Es wird empfohlen, die Aufgabe zur Inventarisierung von Software zu deaktivieren und die Benachrichtigungen des Administrationsservers über gestartete Programme (in den Einstellungen der Richtlinie von Kaspersky Endpoint Security) zu deaktivieren.

Wenn Sie sich entscheiden, PostgreSQL oder Postgres Pro als DBMS zu installieren, stellen Sie sicher, dass Sie ein Kennwort für den Superuser angegeben haben. Wenn das Kennwort nicht angegeben wird, kann sich der Administrationsserver möglicherweise nicht mit der Datenbank verbinden.

Wenn Sie MySQL, MariaDB, PostgreSQL, oder Postgres Pro installieren, verwenden Sie die empfohlenen Einstellungen, um sicherzustellen, dass das DBMS ordnungsgemäß funktioniert.

Wenn Sie PostgreSQL, MariaDB oder MySQL als DBMS verwenden, wird auf der Registerkarte **Ereignisse** möglicherweise eine unvollständige Liste der Ereignisse für das ausgewählte Client-Gerät angezeigt. Dies kommt vor, wenn das DBMS eine sehr große Anzahl von Ereignissen speichert. Sie können die Anzahl der angezeigten Ereignisse auf eine der folgenden Arten erhöhen:

- Nicht benötigte Ereignisse entfernen.
- Speicherdauer für nicht benötigte Ereignisse verkürzen.

Verwenden Sie die Berichte, um eine vollständige Liste der auf dem Administrationsserver für das Gerät protokollierten Ereignisse anzuzeigen.

Adresse des Administrationsservers angeben

Bei der Installation des Administrationsservers muss der DNS-Name oder die statische IP-Adresse des Administrationsservers festgelegt werden. Diese Adresse wird standardmäßig beim Erstellen der Installationspakete des Administrationsagenten verwendet. In Folge kann die Adresse des Hosts des Administrationsservers mithilfe der Kaspersky Security Center Web Console geändert werden. Dabei wird die Adresse jedoch nicht automatisch in den schon erstellten Installationspaketen des Administrationsagenten geändert.

Inaktive Verbindungen aufrechterhalten

Es wird empfohlen, dass Sie die folgenden keepalive-Parameter auf den Geräten konfigurieren, die als Verbindungs-Gateways dienen, um die Verbindungsstabilität zu verbessern:

- `net.ipv4.tcp_keepalive_intvl` gibt an, wie oft keepalive-Nachrichten nach der ersten Nachricht gesendet werden sollen Setzen Sie diesen Parameter auf `1`.
- `net.ipv4.tcp_keepalive_probes` gibt an, wie viele keepalive-Nachrichten ohne Antwort gesendet werden können, bevor die Verbindung als tot gilt. Setzen Sie diesen Parameter auf `10`.
- `net.ipv4.tcp_keepalive_time` gibt an, wie lange nach dem letzten Datenpaket gewartet werden soll, bevor die erste keepalive-Nachricht gesendet wird. Setzen Sie diesen Parameter auf `900`.

So konfigurieren Sie die keepalive-Parameter:

1. Öffnen Sie die Datei /etc/sysctl.conf.
2. Fügen Sie die folgenden Parameterwerte hinzu:

   ```
   net.ipv4.tcp_keepalive_intvl = 1
   net.ipv4.tcp_keepalive_probes = 10
   net.ipv4.tcp_keepalive_time = 900
   ```

3. Führen Sie den folgenden Befehl aus, um die keepalive-Parameter zu aktualisieren:

   ```
   sudo sysctl -p /etc/sysctl.conf
   ```

4. Führen Sie die folgenden Befehle aus, um sicherzustellen, dass die Parameterwerte angewendet wurden:

   ```
   sudo sysctl net.ipv4.tcp_keepalive_intvl
   sudo sysctl net.ipv4.tcp_keepalive_probes
   sudo sysctl net.ipv4.tcp_keepalive_time
   ```

Administrationsagent und die Sicherheitsanwendungen bereitstellen

Um die Geräte in einer Organisation zu verwalten und gegen Sicherheitsbedrohungen zu schützen, müssen Sie auf jedem Gerät den Administrationsagenten und eine Sicherheitsanwendung von Kaspersky installieren.

Weitere Informationen zur Bereitstellung des Schutzes erhalten Sie im Abschnitt Bereitstellung des Administrationsagenten und der Sicherheitsanwendung.

Weitere Informationen zum Schutz mobiler Geräte finden Sie im Abschnitt Verwaltung mobiler Geräte.

Unter Windows XP führt der Administrationsagent folgende Operationen möglicherweise nicht korrekt aus: Das Herunterladen von Updates direkt von den Servern von Kaspersky (als Verteilungspunkt), das Fungieren als KSN-Proxyserver (als Verteilungspunkt) und das Erkennen von Schwachstellen bei Drittanbietern (wenn die Funktion Schwachstellen- und Patch-Management genutzt wird).

Schutz im Netzwerk eines Kundenunternehmens anpassen

Nach dem Abschließen der Installation des Administrationsservers wird die Kaspersky Security Center Web Console gestartet, welche vorschlägt, die Erstkonfiguration mithilfe des Assistenten auszuführen. Während der Ausführung des Schnellstartassistenten in der Stamm-Administrationsgruppe werden die folgenden Richtlinien und Aufgaben erstellt:

- Richtlinie von Kaspersky Endpoint Security
- Gruppenaufgabe zum Update von Kaspersky Endpoint Security
- Gruppenaufgabe zur Untersuchung des Geräts von Kaspersky Endpoint Security
- Richtlinie für den Administrationsagenten
- Aufgabe zur Untersuchung auf Schwachstellen (Aufgabe des Administrationsagenten)
- Aufgabe zur Installation der Updates und zum Schließen von Schwachstellen (Aufgabe des Administrationsagenten)

Die Richtlinien und Aufgaben werden mit den Standardeinstellungen erstellt, die sich möglicherweise als nicht optimal oder sogar untauglich für das vorliegende Unternehmen erweisen. Deshalb ist es erforderlich, die Eigenschaften der erstellten Objekte anzuzeigen erforderlichenfalls manuelle Änderungen vorzunehmen.

Dieser Abschnitt enthält Informationen über die manuelle Konfiguration von Richtlinien, Aufgaben und andere Einstellungen des Administrationsservers sowie Informationen über den Verteilungspunkt, den Aufbau der Struktur der Administrationsgruppen, die Hierarchie von Aufgaben und andere Einstellungen.

Richtlinie für Kaspersky Endpoint Security manuell konfigurieren

Dieser Abschnitt enthält Empfehlungen für das Anpassen der Einstellungen der Richtlinie für Kaspersky Endpoint Security, die vom Schnellstartassistenten erstellt wird. Sie können die Einrichtung im Fenster mit den Richtlinieneigenschaften durchführen.

Beachten Sie beim Bearbeiten einer Einstellung, dass Sie die Einstellung sperren oder entsperren können, um das Ändern ihres Wertes auf einer Workstation zu verbieten oder zuzulassen.

Einstellungen der Richtlinie im Abschnitt "Erweiterter Schutz"

Die vollständige Beschreibung der Einstellungen in diesem Abschnitt finden Sie in der Dokumentation zu Kaspersky Endpoint Security für Windows.

Im Abschnitt **Erweiterter Schutz** können Sie die Verwendung von Kaspersky Security Network für Kaspersky Endpoint Security für Windows anpassen. Sie können auch die Module von Kaspersky Endpoint Security für Windows anpassen. Dazu zählen "Verhaltensanalyse", "Exploit-Prävention", "Programm-Überwachung" und "Rollback von schädlichen Aktionen".

Es wird empfohlen, im Unterabschnitt **Kaspersky Security Network** die Option **Kaspersky Security Network** zu aktivieren. Diese Option unterstützt Sie bei der Umverteilung und Optimierung des Datenverkehrs im Netzwerk. Wenn die Option **Kaspersky Security Network** deaktiviert ist, können Sie die direkte Verwendung von KSN-Servern aktivieren.

Einstellungen der Richtlinie im Abschnitt "Basisschutz"

Die vollständige Beschreibung der Einstellungen in diesem Abschnitt finden Sie in der Dokumentation zu Kaspersky Endpoint Security für Windows.

Es wird empfohlen, dass Sie im Abschnitt **Basisschutz** des Eigenschaftsfensters der Richtlinie die zusätzlichen Einstellungen für die Unterabschnitte **Firewall** und **Schutz vor bedrohlichen Dateien** angeben.

Der Unterabschnitt **Firewall** enthält Einstellungen, mit denen Sie die Netzwerkaktivität von Anwendungen auf den Client-Geräten steuern können. Ein Client-Gerät verwendet ein Netzwerk, dem einer der folgenden Statuswerte zugewiesen ist: öffentlich, lokal oder vertrauenswürdig. Je nach Netzwerkstatus kann Kaspersky Endpoint Security die Netzwerkaktivitäten auf einem Gerät zulassen oder verweigern. Wenn Sie Ihrer Organisation ein neues Netzwerk hinzufügen, müssen Sie ihm einen entsprechenden Netzwerkstatus zuweisen. Wenn das Client-Gerät beispielsweise ein Laptop ist, empfehlen wir, dass dieses Gerät das öffentliche oder vertrauenswürdige Netzwerk verwendet, da der Laptop nicht ausschließlich mit dem lokalen Netzwerk verbunden ist. In dem Unterabschnitt **Firewall** können Sie überprüfen, ob Sie die Statuswerte der in Ihrer Organisation verwendeten Netzwerke korrekt zugewiesen haben.

Um die Liste der Netzwerke zu überprüfen, gehen Sie wie folgt vor:

1. Wechseln Sie in den Richtlinieneinstellungen zu Basisschutz → **Firewall**.
2. Klicken Sie im Block **Verfügbare Netzwerke** auf die Schaltfläche **Einstellungen**.
3. Wechseln Sie im angezeigten Fenster **Firewall** zu der Registerkarte **Netzwerke**, um die Liste der Netzwerke anzuzeigen.

In dem Unterabschnitt **Schutz vor bedrohlichen Dateien** können Sie das Untersuchen von Netzlaufwerken deaktivieren. Das Untersuchen von Netzlaufwerken kann eine erhebliche Belastung auf den Netzlaufwerken darstellen. Daher ist es zweckmäßiger, die Untersuchung unmittelbar auf den Dateiservern auszuführen.

Um die Untersuchung von Netzlaufwerken zu deaktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie in den Richtlinieneinstellungen zu **Basisschutz → Schutz vor bedrohlichen Dateien**.
2. Klicken Sie im Abschnitt **Sicherheitsstufe** auf **Einstellungen**.
3. Deaktivieren Sie neuen Fenster **Schutz vor bedrohlichen Dateien** auf der Registerkarte **Allgemein** das Kontrollkästchen **Alle Netzlaufwerke**.

Einstellungen der Richtlinie im Abschnitt "Allgemeine Einstellungen"

Die vollständige Beschreibung der Einstellungen in diesem Abschnitt finden Sie in der Dokumentation zu Kaspersky Endpoint Security.

Es folgt die Beschreibung der erweiterten Einrichtung anhand von Maßnahmen, die im Eigenschaftenfenster der Richtlinie von Kaspersky Endpoint Security im Abschnitt **Allgemeine Einstellungen** durchgeführt werden sollten.

Abschnitt "Allgemeine Einstellungen", Unterabschnitt "Berichte und Speicher"

Bitte beachten Sie im Abschnitt **Datenübertragung zum Administrationsserver** das Kontrollkästchen **Über gestartete Anwendungen**. Wenn dieses Kontrollkästchen aktiviert ist, werden in der Administrationsserver-Datenbank Informationen über alle Versionen aller Programm-Module auf den Geräten im Unternehmensnetzwerk gespeichert. Diese Informationen können in der Datenbank von Kaspersky Security Center Linux eine erhebliche Größe (mehrere Gigabyte) einnehmen. Wenn daher das Kontrollkästchen **Über die ausgeführten Programme** in der Richtlinie der obersten Ebene noch aktiviert ist, muss es dort deaktiviert werden.

Abschnitt "Allgemeine Einstellungen", Unterabschnitt "Benutzeroberfläche"

Wenn der Bedrohungsschutz im Unternehmensnetzwerk zentral über die Kaspersky Security Center Web Console verwaltet werden soll, müssen Sie die Anzeige der Benutzeroberfläche von Kaspersky Endpoint Security auf den Workstations deaktivieren (Deaktivieren des Kontrollkästchen **Benutzeroberfläche anzeigen** im Abschnitt **Interaktion mit dem Benutzer**) und den Kennwortschutz aktivieren (Aktivieren des Kontrollkästchens **Kennwortschutz aktivieren** im Abschnitt **Kennwortschutz**).

Einstellungen der Richtlinie im Abschnitt "Konfiguration von Ereignissen"

Im Abschnitt **Konfiguration von Ereignissen** muss die Speicherung aller Ereignisse auf dem Administrationsserver mit Ausnahme der nachstehenden deaktiviert werden:

- Auf der Registerkarte **Kritisch**:
  - *Autostart des Programms wurde deaktiviert*
  - *Zugriff verweigert*
  - *Programmstart verboten*
  - *Desinfektion nicht möglich*
  - *Endbenutzer-Lizenzvertrag wurde verletzt*

- *Das Verschlüsselungsmodul konnte nicht geladen werden*
- *Zwei Aufgaben können nicht gleichzeitig gestartet werden*
- *Eine aktive Bedrohung wurde gefunden. Die aktive Desinfektion muss gestartet werden*
- *Netzwerkangriff erkannt*
- *Nicht alle Komponenten wurden aktualisiert*
- *Aktivierungsfehler*
- *Fehler beim Aktivieren des portablen Modus*
- *Fehler bei Interaktion mit Kaspersky Security Center*
- *Fehler beim Deaktivieren des portablen Modus*
- *Fehler beim Ändern der Auswahl der Programmkomponenten*
- *Fehler bei der Anwendung von Regeln zur Verschlüsselung / Entschlüsselung von Dateien*
- *Die Richtlinie kann nicht übernommen werden*
- *Prozess beendet*
- *Netzwerkaktivität verboten*

- Auf der Registerkarte **Funktionsfehler**: *Ungültige Aufgabeneinstellungen. Einstellungen nicht übernommen*
- Auf der Registerkarte **Warnung**:
  - *Selbstschutz ist deaktiviert*
  - *Ungültiger Reserveschlüssel*
  - *Der Benutzer hat die Verschlüsselungsrichtlinie abgelehnt*
- Auf der Registerkarte **Information**: *Programmstart im Testmodus verboten*

Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren

Falls der Administrationsserver als Update-Quelle dient, ist der Zeitplan **Nach dem Download von Updates in die Datenverwaltung** bei aktiviertem Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** der optimale und empfohlene Zeitplan für Gruppenaufgaben zum Update von Kaspersky Endpoint Security.

Wenn Sie auf jedem Verteilungspunkt eine lokale Aufgabe für den Download von Updates von den Servern von Kaspersky in den Speicher erstellt haben, ist für die Gruppenaufgabe zum Update von Kaspersky Endpoint Security ein regelmäßiger Zeitplan optimal und empfohlen. In diesem Fall sollte als Zeitraum für den zufälligen Start 1 Stunde angegeben werden.

Manuelle Konfiguration der Gruppenaufgabe zur Untersuchung des Geräts durch Kaspersky Endpoint Security

Der Schnellstartassistent erstellt die Gruppenaufgabe zur Untersuchung des Geräts. Wenn der automatisch festgelegte Zeitplan für die Gruppenaufgabe zur Untersuchung für Ihr Unternehmen ungeeignet ist, müssen Sie den für diese Aufgabe am besten geeigneten Zeitplan basierend auf den im Unternehmen festgelegten Arbeitsplatzregeln manuell festlegen.

So ist beispielsweise ist für die Aufgabe der Zeitplan **Freitags um 19:00 Uhr starten** mit automatischer zufälliger Streuung ausgewählt und das Kontrollkästchen **Übersprungene Aufgaben starten** ist deaktiviert. Wenn in diesem Fall die Geräte des Unternehmens freitags, um 18:30 Uhr heruntergefahren werden, bedeutet dies, dass die Untersuchungsaufgabe des Geräts niemals ausgeführt wird. In diesem Fall müssen Sie die Gruppenaufgabe zur Untersuchung manuell einrichten.

Aufgabe "Suche nach Schwachstellen und erforderlichen Updates" planen

Der Schnellstartassistent erstellt für den Administrationsagenten die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*. Standardmäßig ist für die Aufgabe der Zeitplan **Dienstag um 19:00 Uhr starten** mit automatischer Randomisierung ausgewählt und das Kontrollkästchen **Übersprungene Aufgaben starten** ist aktiviert.

Wenn die Dienstvorschriften des Unternehmens zu dieser Zeit ein Deaktivieren der Geräte vorsehen, wird die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* nach dem Aktivieren des Geräts (am Mittwochmorgen) ausgeführt. Ein solches Verhalten kann unerwünscht sein, da die Untersuchung auf Schwachstellen eine erhöhte Belastung des Prozessors und des Laufwerkssubsystems des Geräts veranlassen kann. Für einen optimalen Aufgabenzeitplan sollten die im Unternehmen geltenden Regeln und Vorschriften berücksichtigt werden.

Manuelle Konfiguration der Gruppenaufgabe zur Installation von Updates und zum Schließen von Schwachstellen

Der Schnellstartassistent erstellt für den Administrationsagenten die Gruppenaufgabe zur Installation der Updates und zum Schließen von Schwachstellen. Standardmäßig ist der Aufgabenstart täglich um 1:00 Uhr mit zufälliger Verzögerung konfiguriert und die Option **Übersprungene Aufgaben starten** ist deaktiviert.

Wenn die Dienstvorschriften des Unternehmens während der Nacht ein Deaktivieren der Geräte vorsehen, wird die Aufgabe zur Installation der Updates niemals ausgeführt. Es ist erforderlich, den optimalen Zeitplan der Aufgabe zur Untersuchung auf Schwachstellen ausgehend von den im Unternehmen geltenden Dienstvorschriften festzulegen. Ferner muss berücksichtigt werden, dass infolge der Installation der Updates ein Neustart des Geräts erforderlich sein kann.

Aufbau der Struktur von Administrationsgruppen und Zuweisung von Verteilungspunkten

Die Struktur der Administrationsgruppen in Kaspersky Security Center Linux erfüllt folgende Funktionen:

- Gültigkeitsbereich der Richtlinien festlegen.

  Mithilfe von Richtlinienprofilen existiert eine alternative Möglichkeit, um die notwendigen Einstellungen auf den Geräten anzuwenden. In diesem Fall wird der Umfang der Richtlinien z. B. mithilfe von Geräte-Tags oder Benutzerrollen festgelegt.

- Gültigkeitsbereich der Gruppenaufgaben festlegen.

  Es gibt eine Methode zur Festlegung des Gültigkeitsbereichs der Gruppenaufgaben, die nicht auf der Hierarchie der Administrationsgruppen basiert: die Nutzung von Aufgaben für die Geräteauswahlen und eine Reihe von Geräten.

- Festlegung der Zugriffsrechte auf die Geräte, die virtuellen und sekundären Administrationsserver.

- Weist Verteilungspunkte zu.

Beim Aufbau der Struktur der Administrationsgruppen muss für eine optimale Bestimmung der Verteilungspunkte die Netzwerktopologie des Unternehmens berücksichtigt werden. Die optimale Zuordnung der Verteilungspunkte ermöglicht eine Verringerung des Netzwerkverkehrs innerhalb des Unternehmensnetzwerks.

Abhängig von der planmäßigen Struktur des MSP-Kunden und der Topologie der Netzwerke können die folgenden typischen Konfigurationen für die Struktur der Administrationsgruppen unterschieden werden:

- Einzelbüro

- Mehrere kleine, eigenständige Büros

Typische Konfiguration des MSP-Kunden: Einzelbüro

In einer typischen Einzelbüro-Konfiguration befinden sich alle Geräte im Netzwerk des Unternehmens und können einander "sehen". Das Netzwerk des Unternehmens kann aus mehreren ausgewählten Teilen (der Netzwerke oder der Netzwerksegmente) bestehen, die über enge Kanäle verbunden sind.

Es sind die folgenden Methoden für den Aufbau der Struktur der Administrationsgruppen möglich:

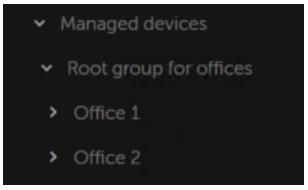
- Aufbau der Struktur der Administrationsgruppen unter Berücksichtigung der Netztopologie. Die Struktur der Administrationsgruppen muss die Netztopologie nicht unbedingt genau widerspiegeln. Es ist ausreichend, wenn den einzelnen Teilen des Netzwerkes bestimmte Administrationsgruppen entsprechen. Die Verteilungspunkte können automatisch bestimmt oder manuell zugewiesen werden.

- Aufbau der Struktur der Administrationsgruppen, in der die Netztopologie nicht widergespiegelt wird. In diesem Fall müssen Sie die automatische Bestimmung der Verteilungspunkte deaktivieren und dann für die Stammadministrationsgruppe in jedem ausgewählten Teil des Netzwerkes ein oder mehrere Geräte als Verteilungspunkte bestimmen, beispielsweise für die Gruppe **Verwaltete Geräte**. Alle Verteilungspunkte befinden sich dann auf einer Ebene und haben den identischen Gültigkeitsbereich, der alle Geräte im Netzwerk des Unternehmens umfasst. Jeder der Administrationsagenten wird in diesem Fall mit dem Verteilungspunkt verbunden, zu dem die Route am kürzesten ist. Die Route zum Verteilungspunkt kann mithilfe der Tools "tracert" oder "traceroute" bestimmt werden.

Typische Konfiguration des MSP-Kunden: Mehrere kleine, eigenständige Büros

Diese typische Konfiguration entspricht einigen kleinen Remote-Büros, die beispielsweise über das Internet mit dem Hauptbüro verbunden sind. Jedes der Remote-Büros befindet sich hinter einer NAT. Das bedeutet, dass ein Remote-Büro nicht mit einem anderen verbunden werden kann und die Büros voneinander isoliert sind.

Diese Konfiguration muss in der Struktur der Administrationsgruppen widergespiegelt werden: für jedes Remote-Büro muss eine separate Administrationsgruppe erstellt werden (entspr. Gruppen **Büro 1**, **Büro 2** auf der nachfolgenden Abbildung).



Die Remote-Büros werden in der Struktur der Administrationsgruppen abgebildet.

Für jede Administrationsgruppe, die einem Büro entspricht, müssen ein oder mehrere Verteilungspunkte festgelegt werden. Als Verteilungspunkte müssen Geräte des Remote-Büros bestimmt werden, die genug freien Platz auf dem Datenträger haben. Die Geräte, die sich beispielsweise in der Gruppe **Büro 1** befinden, wenden sich an die Verteilungspunkte, die für die Administrationsgruppe **Büro 1** bestimmt wurden.

Wenn einige Benutzer samt ihren Laptops physisch zwischen Büros wechseln, müssen in jedem Remote-Büro zusätzlich zu den oben erwähnten Verteilungspunkten zwei oder mehrere Geräte ausgewählt und als Verteilungspunkte für die Administrationsgruppe der obersten Ebene bestimmt werden (Gruppe **Stammgruppe für die Büros** in der obigen Abbildung).

Beispiel: Es gibt einen Laptop, der sich in der Administrationsgruppe **Büro 1** befindet, aber physisch in ein Büro gebracht wird, das der Gruppe **Büro 2** entspricht. Nach dem Ortswechsel versucht der Administrationsagent auf dem Laptop, sich an die Verteilungspunkte zu wenden, die zur Gruppe **Büro 1** gehören. Diese Verteilungspunkte erweisen sich allerdings als nicht verfügbar. Dann beginnt der Administrationsagent, sich an die Verteilungspunkte zu wenden, die für die Gruppe **Stammgruppe für die Büros** bestimmt wurden. Da die Remote-Büros voneinander isoliert sind, werden von allen Verteilungspunkten, die für die Administrationsgruppe **Stammgruppe für die Büros** bestimmt wurden, nur die Zugriffe des Administrationsagenten auf die Verteilungspunkte erfolgreich sein, die für die Gruppe **Büro 2** bestimmt wurden. Das bedeutet, dass der Laptop zwar in der Administrationsgruppe bleibt, die dem ursprünglichen Büro entspricht, aber die Verteilungspunkte jenes Büros verwendet, in dem er sich in diesen Moment physisch befindet.

Richtlinienhierarchie, Verwendung von Richtlinienprofilen

Dieser Abschnitt enthält Informationen über Besonderheiten der Anwendung von Richtlinien auf Geräte in Administrationsgruppen. Dieser Abschnitt enthält auch Informationen zu Richtlinienprofilen.

Hierarchie der Richtlinien

In Kaspersky Security Center Linux sind Richtlinien für die Angabe eines identischen Satzes von Einstellungen auf mehreren Geräten vorgesehen. Beispielsweise betrifft der Gültigkeitsbereich der Richtlinie des Programms P, die für die Administrationsgruppe G bestimmt ist, die verwalteten Geräte mit dem installierten Programm P in der Administrationsgruppe G und allen ihren Untergruppen, mit Ausnahme jener Untergruppen, in deren Eigenschaften das Kontrollkästchen **Aus übergeordneter Gruppe erben** deaktiviert ist.

Eine Richtlinie unterscheidet sich von den lokalen Einstellungen durch das Vorhandensein von Schloss-Symbolen ( ) neben den in ihr enthaltenen Einstellungen. Ein aktiviertes "Schloss" in den Richtlinieneigenschaften bedeutet, dass die entsprechende Einstellung (bzw. die Einstellungsgruppe) erstens beim Erstellen der wirksamen Einstellungen verwendet werden soll, und zweitens auf die niedrigere Richtlinie angewendet werden soll.

Das Erstellen der auf dem Gerät geltenden Einstellungen kann auf folgende Weise realisiert werden: Aus der Richtlinie die Werte der Einstellungen mit nicht aktiviertem Schloss übernehmen und die Werte der lokalen Einstellungen darüber speichern. Dann werden über die erhaltenen Werte die aus der Richtlinie übernommenen Werte der Einstellungen mit aktiviertem Schloss gespeichert.

Die Richtlinien ein und desselben Programms beeinflussen einander gegenseitig gemäß der Hierarchie der Administrationsgruppen: die Einstellungen mit dem aktivierten Schloss aus der höher liegenden Richtlinien überschreiben die gleichnamigen Einstellungen aus der niedriger liegenden Richtlinie.

Es existiert eine besondere Art von Richtlinie, nämlich die Richtlinie für mobile Benutzer. Diese Richtlinie tritt auf einem Gerät in Kraft, wenn das Gerät in den Modus für mobile Benutzer wechselt. Mobile Richtlinien gelten gemäß der Hierarchie der Administrationsgruppen nicht auf andere Richtlinien.

Richtlinienprofile

Die Anwendung der Richtlinien auf den Geräten nur aufgrund der Hierarchie der Administrationsgruppen ist in vielen Fällen ungeeignet. Es kann erforderlich werden, in verschiedenen Administrationsgruppen mehrere Kopien einer Richtlinie zu erstellen, die sich ein bis zwei Einstellungen unterscheiden, und im Folgenden den Inhalt dieser Richtlinien manuell zu synchronisieren.

Um Ihnen zu helfen, solche Probleme zu vermeiden, unterstützt Kaspersky Security Center Linux *Richtlinienprofile*. Ein Richtlinienprofil ist eine benannte Teilmenge von Richtlinieneinstellungen. Diese Teilmenge wird auf Zielgeräten gemeinsam mit der Richtlinie verteilt und ergänzt sie unter einer bestimmten Bedingung, die als *Profilaktivierungsbedingung* bezeichnet wird. Profile enthalten nur jene Einstellungen, die sich von "zugrundeliegenden" Richtlinie unterscheiden, die auf dem Client-Gerät (Computer, mobiles Gerät) gilt. Bei der Aktivierung des Profils werden die Einstellungen der bis zur Aktivierung des Profils auf dem Gerät geltenden Richtlinie geändert. Diese Einstellungen nehmen die im Profil festgelegten Werte an.

Richtlinienprofile haben derzeit folgende Einschränkungen:

- Die Richtlinie darf nicht mehr als 100 Profile enthalten.
- Ein Richtlinienprofil kann keine anderen Profile enthalten.
- Ein Richtlinienprofil darf keine Benachrichtigungseinstellungen enthalten.

Zusammensetzung des Profils

Ein Richtlinienprofil enthält die folgenden Bestandteile:

- Name. Profile mit identischen Namen wirken sich auf einander gemäß der Hierarchie der Administrationsgruppen mit den allgemeinen Regeln aus.
- Teilmenge der Richtlinieneinstellungen. Im Unterschied zur Richtlinie, in der alle Einstellungen enthalten sind, enthält ein Profil nur jene Einstellungen, die wirklich erforderlich sind (für die ein Schloss definiert ist).

- Die Aktivierungsbedingung ist ein logischer Ausdruck über den Eigenschaften des Geräts. Das Profil ist nur aktiv (ergänzt die Richtlinie), wenn die Aktivierungsbedingung des Profils erfüllt ist. In den übrigen Fällen ist das Profil inaktiv und wird ignoriert. Am logischen Ausdruck können die folgenden Geräteigenschaften teilnehmen:

  - Status des Modus für mobile Benutzer.

  - Die Eigenschaften der Netzwerkumgebung – der Name der aktiven Regel zur Verbindung des Administrationsagenten.

  - Vorhandensein oder Abwesenheit der angegebenen Tags auf dem Gerät.

  - Der Standort des Geräts im Active Directory-Einheit: explizit (das Gerät befindet sich unmittelbar in der angegebenen Organisationseinheit) oder implizit (das Gerät befindet sich in einer Organisationseinheit, die sich auf einer beliebigen Verschachtelungsebene innerhalb der angegebenen Organisationseinheit befindet).

  - Zugehörigkeit des Geräts zur Sicherheitsgruppe Active Directory (explizit oder implizit).

  - Zugehörigkeit des Gerätebesitzers zur Sicherheitsgruppe Active Directory (explizit oder implizit).

- Kontrollkästchen zum Deaktivierens des Profils. Deaktivierten Profile werden immer ignoriert, ihre Aktivierungsbedingungen werden nicht auf den Wahrheitsgehalt geprüft.

- Priorität des Profils. Die Aktivierungsbedingungen der Profile sind unabhängig, deshalb können mehrere Profile sofort gleichzeitig aktiviert werden. Wenn sich die aktiven Profile Einstellungssätze enthalten, die sich überschneiden, entstehen keine Probleme. Wenn jedoch zwei aktive Profile verschiedene Werte für ein und dieselbe Einstellung enthalten, entsteht eine Mehrdeutigkeit. Diese Mehrdeutigkeit wird mithilfe der Prioritäten der Profile entfernt: der Wert für die mehrdeutigen Variablen dem Profil mit der höheren Priorität (jenem Profil, das sich weiter oben in der Liste der Profile befindet) entnommen.

Verhalten der Profile bei der gegenseitigen Aktion der Richtlinien gemäß der Hierarchie

Gleichnamige Profile werden gemäß den Regeln zur Vereinigung von Richtlinien zusammengeführt. Profile der oberen Richtlinie haben gegenüber den Profilen der unteren Richtlinie Priorität. Wenn in "oberen" Richtlinie eine Änderung der Einstellungen verboten ist (die Schaltfläche Schloss wurde geklickt), werden in der "unteren" Richtlinie Aktivierungsbedingungen des Profils aus der "oberen" Richtlinie verwendet. Wenn in der "oberen" Richtlinie die Änderung der Einstellungen erlaubt ist, werden die Aktivierungsbedingungen des Profils aus der "unteren" Richtlinie verwendet.

Da das Richtlinienprofil in den Aktivierungsbedingungen die Eigenschaft **Gerät im autonomen Modus** enthalten kann, wird die Funktionalität der Richtlinien für mobile Benutzer vollständig durch die Profile ersetzt und nicht länger unterstützt.

Die Richtlinie für eigenständige Benutzer kann Profile enthalten, deren Aktivierung jedoch erst erfolgen kann, wenn das Gerät in den Modus für mobile Benutzer wechselt.

Aufgaben

Kaspersky Security Center Linux verwaltet die auf Geräten installierten Sicherheitsanwendungen von Kaspersky durch das Erstellen und Starten von *Aufgaben*. Die Aufgaben ermöglichen Installation, Start und Beenden von Anwendungen, Untersuchung von Dateien, Datenbanken-Update und Aktualisierung der Anwendungsmodule sowie Ausführung anderer Aktionen mit den Anwendungen.

Aufgaben für eine bestimmte Anwendung können nur erstellt werden, sofern das Verwaltungs-Plug-in für diese Anwendung installiert ist.

Aufgaben können auf dem Administrationsserver und auf Geräten ausgeführt werden.

Die folgenden Aufgaben werden auf dem Administrationsserver ausgeführt:

- Berichte automatisch versenden
- Updates in die Datenverwaltung des Administrationsservers herunterladen
- Backup der Daten des Administrationsservers anlegen
- Datenbank bedienen

Die folgenden Typen von Aufgaben werden auf Geräten ausgeführt:

- *Lokale Aufgaben* sind Aufgaben, die auf einem bestimmten Gerät ausgeführt werden.

  Lokale Aufgaben können nicht nur vom Administrator mithilfe von Kaspersky Security Center Web Console geändert werden, sondern auch vom Benutzer des Remote-Gerätes (beispielsweise in der Benutzeroberfläche der Sicherheits-Anwendungen). Wenn eine lokale Aufgabe gleichzeitig sowohl vom Administrator als auch vom Benutzer auf dem verwalteten Gerät geändert wurde, treten jene Änderungen in Kraft, die vom Administrator mit höherer Priorität ausgeführt wurden.

- *Gruppenaufgaben* sind Aufgaben, die auf allen Geräten einer bestimmten Gruppe ausgeführt werden.

  Soweit in den Aufgabeneigenschaften nicht anders festgelegt, betrifft eine Gruppenaufgabe auch alle Untergruppen der ausgewählten Gruppe. Eine Gruppenaufgabe betrifft (optional) auch Geräte, die mit den sekundären und virtuellen Administrationsservern in der Gruppe und den Untergruppen verbunden sind.

- *Globale Aufgaben* sind Aufgaben, die auf einem Satz von Geräten ausgeführt werden, und zwar unabhängig davon, ob sie zu einer Gruppe gehören.

Sie können für jede Anwendung eine beliebige Anzahl von Gruppenaufgaben, globalen Aufgaben oder lokalen Aufgaben erstellen.

Sie können die Aufgabeneinstellungen ändern, den Fortschritt von Aufgaben verfolgen, und Aufgaben kopieren, exportieren, importieren und löschen.

Eine Aufgabe wird auf einem Gerät nur dann gestartet, wenn die Anwendung gestartet wurde, für das diese Aufgaben erstellt worden waren.

Ergebnisse von Aufgaben werden im Syslog-Ereignisprotokoll und im Ereignisprotokoll von Kaspersky Security Center Linux sowohl zentral auf dem Administrationsserver als auch lokal auf jedem Gerät gespeichert.

Geben Sie in den Einstellungen der Aufgaben keine vertraulichen Daten an. Dazu gehört z. B. das Kennwort des Domänenadministrators.

Verschiebungsregeln für Geräte

Es wird empfohlen, die Verteilung von Geräten auf Administrationsgruppen mithilfe der *Regeln für das Verschieben von Geräten* zu automatisieren. Die Regel zum Verschieben besteht aus drei Hauptteilen: dem Namen, der Ausführungsbedingung (logischer Ausdruck über die Attribute des Geräts) und der Zieladministrationsgruppe. Die Regel verschiebt das Gerät in die Zieladministrationsgruppe, wenn die Attribute des Geräts die Bedingung für die Regelausführung erfüllen.

Alle Regeln für das Verschieben von Geräten haben Prioritäten. Der Administrationsserver prüft die Attribute des Geräts auf Übereinstimmung mit der Bedingung für die jeweilige Regelausführung in abnehmender Priorität der Regeln. Wenn die Attribute des Geräts die Bedingungen für die Regelausführung erfüllen, wird das Gerät in die Zielgruppe verschoben und beendet daraufhin die Verarbeitung der Regeln für das betreffende Gerät. Wenn die Attribute des Geräts sofort einigen Regeln entsprechen, wird das Gerät in die Zielgruppe jener Regel verschoben, welche die höchste Priorität hat (in der Liste der Regeln weiter oben steht).

Die zum Geräte verschieben können implizit erstellt werden. Beispielsweise kann in den Eigenschaften des Installationspakets oder der Aufgabe zur Remote-Installation die Administrationsgruppe angegeben werden, in die das Gerät gelangen soll, nachdem darauf der Administrationsagent installiert wurde. Regeln zum Verschieben von Geräten kann der Administrator von Kaspersky Security Center Linux auch explizit im Abschnitt **Asset-Verwaltung** → **Verschiebungsregeln** erstellen.

Die Regel zum Verschiebung ist standardmäßig für die einmalige erstmalige Verteilung der Geräte auf die Administrationsgruppen vorgesehen. Die Regel verschiebt die Geräte, die sich in der Gruppe für nicht zugeordnete Geräte befinden, nur einmal. Wenn ein Gerät von dieser Regel einmal verschoben wurde, wird es nicht nochmals von der Regel verschoben, selbst wenn das Gerät manuell erneut in die Gruppe für nicht zugeordnete Geräte verschoben wird. Dies ist die empfohlene Art der Nutzung der Regeln zum Verschieben.

Es können Geräte verschoben werden, die sich bereits in Administrationsgruppen befinden. Dazu muss in den Eigenschaften der Regel das Kontrollkästchen **Nur Geräte verschieben, die keiner Administrationsgruppe angehören** deaktiviert werden.

Durch die Existenz von Regeln zum Verschieben, die auf Geräte gelten, die bereits in die Administrationsgruppen verschoben wurden, steigt die Belastung auf dem Administrationsserver erheblich.

In den Eigenschaften von automatisch erstellten Verschiebungsregeln ist das Kontrollkästchen **Nur Geräte verschieben, die keiner Administrationsgruppe angehören** gesperrt. Diese Regeln werden erstellt, wenn Sie die Aufgabe *Remote-Installation einer Anwendung* hinzufügen oder ein autonomes Installationspaket erstellen.

Es kann eine Regel zum Verschieben erstellt werden, die auf einem Gerät mehrfach ausgeführt werden kann.

Es wird dringend empfohlen, Szenarien zu vermeiden, bei denen ein verwaltetes Gerät mehrfach aus einer Gruppe in eine andere verschoben wird (z. B. um eine besondere Richtlinie auf das Gerät anzuwenden, eine spezielle Gruppenaufgabe zu starten oder das Gerät über einen bestimmten Verteilungspunkt zu aktualisieren).

Solche Szenarien werden nicht unterstützt, da sie die Belastung des Administrationsservers und den Datenverkehr in extremem Ausmaß erhöhen. Diese Szenarien stehen ferner in Konflikt mit den Betriebsprinzipien von Kaspersky Security Center Linux (insbesondere im Bereich von Zugriffsrechen, Ereignissen und Berichten). Es müssen andere Lösungen gesucht werden, zum Beispiel durch Verwendung der Richtlinienprofile, der Aufgaben für Geräteauswahlen und der Zuweisung von Administrationsagenten entsprechend dem Standardszenario.

Software-Kategorisierung

Das wichtigste Tool zur Kontrolle des Starts von Apps sind die *Kategorien von Kaspersky* (im Weiteren auch *KL-Kategorien*). Die KL-Kategorien erleichtern dem Administrator von Kaspersky Security Center Linux die Aufrechterhaltung der Kategorisierung der Software und verringern den Umfang des Datenverkehrs, der an die verwalteten Geräte übergeben wird.

Benutzerdefinierte Kategorien müssen nur für Programme erstellt werden, die nicht unter eine KL-Kategorie fallen (beispielsweise für Programme, die auf Bestellung entwickelt wurden). Die benutzerdefinierten Kategorien werden auf der Grundlage der Programmpakete (MSI) oder auf der Grundlage des Ordners mit den Installationspaketen erstellt.

Falls es eine umfangreiche ergänzte Software-Sammlung gibt, die mithilfe der KL-Kategorien kategorisiert ist, kann es zweckmäßig sein, eine automatisch aktualisierte Kategorie zu erstellen. Eine solche Kategorie wird bei der Änderung des Ordners mit den Programmpaketen automatisch mit den Prüfsummen der ausführbaren Dateien ergänzt.

Verschieben ins Backup und Wiederherstellen der Einstellungen des Administrationsservers

Für das Verschieben der Einstellungen des Administrationsservers und der von ihm verwendeten Datenbank ins Backup ist die Aufgabe zum Verschieben ins Backup und das Tool klbackup vorgesehen. Die Backup-Kopie umfasst alle Haupteinstellungen und Objekte des Administrationsservers: die Zertifikate des Administrationsservers, die Primärschlüssel zur Verschlüsselung der Laufwerke der verwalteten Geräte, die Lizenzschlüssel, die Struktur der Administrationsgruppen mit sämtlichem Inhalt, die Aufgaben, die Richtlinien und mehr. Mit einer Backup-Kopie kann die Funktionsfähigkeit eines Administrationsservers schnellstmöglich wiederhergestellt werden, was wenige Minuten oder bis zu zwei Stunden dauern kann.

Bei einer fehlenden Backup-Kopie kann eine Störung zum unwiederbringlichen Verlust der Zertifikate und aller Einstellungen des Administrationsservers führen. Kaspersky Security Center Linux muss dann erneut konfiguriert werden und die erstmalige Bereitstellung des Administrationsagenten im Netzwerk des Unternehmens muss erneut ausgeführt werden. Außerdem gehen auch alle Primärschlüssel zur Verschlüsselung der Laufwerke der verwalteten Geräte verloren, was das Risiko eines unwiederbringlichen Verlustes der verschlüsselten Daten auf den Geräten mit Kaspersky Endpoint Security mit sich bringt. Auf das regelmäßige Erstellen von Backup-Kopien des Administrationsservers mithilfe der Standardaufgabe zum Verschieben ins Backup darf keinesfalls verzichtet werden.

Der Schnellstartassistent erstellt die Aufgabe zum Anlegen eines Backups der Einstellungen des Administrationsservers mit einem täglichen Start um 4:00 Uhr morgens. Gespeichert werden die Backup-Kopien standardmäßig im Ordner /var/opt/kaspersky/KSC_Backups*.

Da eine Backup-Kopie wichtige Daten enthält, ist in der Aufgabe zum Verschieben ins Backup und im Tool klbackup der Schutz der Backup-Kopien durch ein Kennwort vorgesehen. Standardmäßig wird die Aufgabe zum Verschieben ins Backup mit einem leeren Kennwort erstellt. Das Kennwort muss in den Eigenschaften der Aufgabe zum Verschieben ins Backup unbedingt festgelegt werden. Wenn diese Forderung nicht erfüllt wird, führt das dazu, dass die Schlüssel der Zertifikate des Administrationsservers, die Schlüssel für die Lizenzen und die Primärschlüssel zur Verschlüsselung der Laufwerke der verwalteten Geräte nicht verschlüsselt sind.

Neben dem regelmäßigen Verschieben ins Backup muss auch eine Backup-Kopie aller wichtiger Änderungen erstellt werden, darunter auch vor dem Update des Administrationsservers auf die neue Version und vor der Installation der Patches des Administrationsservers.

Die Wiederherstellung aus der Backup-Kopie wird mithilfe des Tools klbackup mit der gerade erst installierten und funktionsfähigen Instanz des Administrationsservers jener Version durchgeführt, für die eine Backup-Kopie erstellt wurde (oder neuer).

Die Instanz des Administrationsservers, auf der die Wiederherstellung ausgeführt werden soll, muss ein DBMS desselben Typs und derselben Version oder höher verwenden. Die Version des Administrationsservers kann gleich (mit einem ähnlichen oder neueren Patch) oder neuer sein.

In diesem Abschnitt werden typische Szenarien für die Wiederherstellung der Einstellungen und der Objekte des Administrationsservers beschrieben.

Ein Gerät mit dem Administrationsserver ist ausgefallen

Wenn das Gerät mit dem Administrationsserver infolge einer Störung außer Betrieb ist, wird empfohlen, wie folgt vorzugehen:

- Dem neuen Administrationsserver muss der gleiche DNS-Name zugewiesen werden.

  Wenn bei der Bereitstellung des Administrationsagenten eine statische IP-Adresse im Installationspaket des Administrationsagenten angegeben war, müssen Sie die gleiche IP-Adresse auch einem neuen Administrationsserver zuordnen. Alternativ können Sie die Verbindungsadresse verwenden, die den Administrationsserver bestimmt, mit dem der Administrationsagent eine Verbindung herstellt (diese Adresse kann auf verwalteten Geräten mithilfe des Tools "klnagchk" ermittelt werden).

- Geben Sie in der IAM-Konfigurationsdatei `var/opt/kaspersky/klnagent_srv/iam/iam_config.yaml` für den Parameter `sserver_iam.ksc_address` die gleiche Administrationsserver-Adresse an, die als alternativer Antragstellername (SAN) im bisher verwendeten Zertifikat des Administrationsservers angegeben ist. Weitere Informationen dazu finden Sie im folgenden Artikel: Adresse des Administrationsservers zur Konfiguration des IAM-Servers hinzufügen.

- Administrationsserver unter Verwendung eines DBMS desselben Typs und derselben oder einer neueren Version installieren. Es kann dieselbe Version des Servers mit demselben oder einem neueren Patch, oder eine neuere Version installiert werden. Nach der Installation muss keine Erstkonfiguration mithilfe des Assistenten ausgeführt werden.

- Starten Sie das Tool "klbackup" und führen Sie die Wiederherstellung durch. Installieren Sie die Web Console nach erfolgreicher Wiederherstellung neu.

Die Einstellungen des Administrationsservers oder der Datenbank sind beschädigt

Wenn der Administrationsserver infolge der Beschädigung der Einstellungen oder der Datenbank funktionsunfähig wurde (beispielsweise wegen eines Stromausfalls), wird empfohlen, das folgende Szenario für die Wiederherstellung zu verwenden:

1. Untersuchung des Dateisystems auf dem betroffenen Gerät durchführen.

2. Funktionsunfähige Version des Administrationsservers deinstallieren.

3. Administrationsserver unter Verwendung eines DBMS desselben Typs und derselben oder einer neueren Version erneut installieren. Es kann dieselbe Version des Servers mit demselben oder einem neueren Patch, oder eine neuere Version installiert werden. Nach der Installation muss keine Erstkonfiguration mithilfe des Assistenten ausgeführt werden.

4. Starten Sie das Tool "klbackup" und führen Sie die Wiederherstellung durch.

Es ist unmöglich, den Administrationsserver auf andere Weise als mit dem Standardtool klbackup wiederherzustellen.

In sämtlichen Fälle der Wiederherstellung des Administrationsservers mithilfe von Drittanbieter-Programmen kommt es unvermeidlich zu einer Desynchronisierung der Daten in den Knoten des verteilten Programms Kaspersky Security Center Linux und in der Folge zu einer inkorrekten Ausführung des Programms.

Über Verbindungsprofile für mobile Benutzer

Bei der Arbeit der mobilen Benutzer, die Laptops (im Weiteren auch "Geräte") verwenden, kann es erforderlich sein, die Verbindungsmethode mit dem Administrationsserver zu ändern oder abhängig von aktuellen Standort des Geräts im Netzwerk zwischen Administrationsservern umzuschalten.

Nutzung verschiedener Adressen ein- und desselben Administrationsservers

Die Geräte mit installiertem Administrationsagenten können in unterschiedlichen Zeiträumen sowohl aus dem internen Netzwerk des Unternehmens als auch aus dem Internet mit dem Administrationsserver verbunden werden. In dieser Situation kann es erforderlich sein, dass der Administrationsagent verschiedene Adressen für die Verbindung mit dem Administrationsserver verwendet: die externe Adresse des Servers bei der Verbindung aus dem Internet und die interne Adresse des Servers bei der Verbindung aus dem internen Netzwerk.

Dazu müssen Sie ein Profil (zur Verbindung mit dem Administrationsserver aus dem Internet) zur Richtlinie des Administrationsagenten hinzufügen. Fügen Sie das Profil in den Richtlinieneigenschaften (Abschnitt **Konnektivität**, Unterabschnitt **Verbindungsprofile**) hinzu. Deaktivieren Sie im Fenster für die Profilerstellung die Option **Nur für Update-Download verwenden** und aktivieren Sie die Option **Verbindungseinstellungen mit den Einstellungen für den Administrationsserver synchronisieren, die in diesem Profil angegeben sind**. Wenn für den Zugriff auf den Administrationsserver ein Verbindungs-Gateway verwendet wird (beispielsweise in einer Konfiguration von Kaspersky Security Center Linux vom Typ Zugriff aus dem Internet: Administrationsagent als Verbindungs-Gateway in der demilitarisierten Zone), muss im Verbindungsprofil die Adresse des Verbindungs-Gateways im entsprechenden Feld angegeben werden.

Umschaltung zwischen Administrationsservern in Abhängigkeit vom aktuellen Netzwerk

Wenn es im Unternehmen mehrere Büros mit verschiedenen Administrationsservern gibt und zwischen ihnen ein Teil der Geräte mit installiertem Administrationsagenten verschoben wird, ist es erforderlich, dass der Administrationsagent mit dem Administrationsserver des lokalen Netzwerkes jenes Büros verbunden wird, in dem sich das Gerät befindet.

In diesem Fall ist es erforderlich, in den Eigenschaften der Richtlinie des Administrationsagenten das Profil für Verbindung mit Administrationsserver für jedes der Büros mit Ausnahme des Büros zu erstellen, in dem sich der Home-Administrationsserver befindet. In den Verbindungsprofilen müssen die Adressen der entsprechenden Administrationsserver angegeben werden und die Option **Nur für Update-Download verwenden** entweder aktiviert oder deaktiviert werden:

- Aktivieren Sie die Option, wenn es erforderlich ist, dass sich der Administrationsagent mit dem Home-Administrationsserver synchronisiert und der lokale Server nur für den Update-Download verwendet wird.
- Deaktivieren Sie diese Option, wenn erforderlich ist, dass der Administrationsagent den lokalen Administrationsserver vollständig verwaltet.

Des Weiteren müssen die Bedingungen für die Umschaltung auf die erstellten Profile angepasst werden: mindestens eine Bedingung für jedes Büro, mit Ausnahme des "Home-Office". Der Sinn jeder solchen Bedingung besteht in der Sichtbarkeit der büroeigenen Details in der Netzwerkumgebung. Wenn eine Bedingung erfüllt wird, erfolgt die Aktivierung des entsprechenden Profils. Trifft keine der Bedingungen zu, wird der Administrationsagent auf den Home-Administrationsserver umgeschaltet.

Über das Umschalten eines Administrationsagenten auf einen anderen Administrationsserver

In Kaspersky Security Center Linux besteht die Möglichkeit, den Administrationsagenten eines Client-Geräts bei einer Änderung der folgenden Netzwerkeigenschaften auf andere Administrationsserver umzuschalten:

- **Bedingung für die DHCP-Serveradresse** – Änderung der IP-Adresse für den DHCP-Server (Dynamic Host Configuration Protocol) im Netzwerk.

  Die Einstellung **Bedingung für die DHCP-Serveradresse** ist derzeit nicht verfügbar.

- **Bedingung für die standardmäßige Adresse des Verbindungs-Gateways** – Änderung des Standard-Gateways im Netzwerk.
- **Bedingung für DNS-Domäne** – Änderung des DNS-Suffixes im Subnetz.
- **Bedingung für die DNS-Serveradresse** – Änderung der IP-Adresse für den DNS-Server im Netzwerk.
- **Bedingung für die WINS-Serveradresse** – Änderung der IP-Adresse für den WINS-Server im Netzwerk. Diese Einstellung ist nur auf Windows-Geräten verfügbar.
- **Bedingung für die Namensauflösung** – Änderung des DNS- oder NetBIOS-Namens des Client-Geräts.
- **Bedingung für Subnetz** – Änderung der Adresse und Subnetzmaske.
- **Bedingung für die Erreichbarkeit der Windows-Domäne** – Änderung des Status der Windows-Domäne, mit der das Client-Gerät verbunden ist. Diese Einstellung ist nur auf Windows-Geräten verfügbar.
- **Bedingung für Verfügbarkeit der SSL-Verbindungsadresse** – Das Client-Gerät kann oder kann nicht (in Abhängigkeit der von Ihnen gewählten Option) eine SSL-Verbindung zu einem Server (Name:Port) herstellen. Sie müssen einen dedizierten Server und eine Software verwenden, die hohen Auslastungen und häufigen Verbindungsanfragen des Administrationsagenten gewachsen ist. Geben Sie nicht den Port des Administrationsservers an. Sie können für jeden Server ein zusätzliches SSL-Zertifikat hinzufügen. In diesem Fall verifiziert der Administrationsagent das Serverzertifikat zusätzlich zur Prüfung auf eine mögliche SSL-Verbindung. Wenn das Zertifikat nicht übereinstimmt, schlägt die Verbindung fehl.

Bei der Installation des Administrationsagenten werden die ursprünglichen Verbindungseinstellungen des Administrationsagenten mit dem Administrationsserver eingegeben. Sobald die Regeln für die Umstellung des Administrationsagenten mit anderen Administrationsservern definiert wurden, reagiert der Agent auf die Änderungen der Netzwerkeigenschaften folgendermaßen:

- Wenn die Netzwerkeigenschaften einer der erstellten Regeln entsprechen, wird der Administrationsagent mit dem in der Regel vorgegebenen Administrationsserver verbunden. Die auf den Client-Geräten installierten Anwendungen wechseln zu den Richtlinien für mobile Benutzer, wenn dies durch eine Regel vorgegeben wurde.

- Wird keine Regel ausgeführt, wird der Administrationsagent auf die ursprünglichen Verbindungseinstellungen mit dem Administrationsserver zurückgesetzt, die bei der Installation vorgegeben wurden. Die auf den Client-Geräten installierten Programme werden auf die aktiven Richtlinien zurückgesetzt.

- Ist der Administrationsserver nicht verfügbar, verwendet der Administrationsagent die Richtlinien für mobile Benutzer.

Der Administrationsagent verwendet die Richtlinie für mobile Benutzer nur dann, wenn die Option **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist** in den Einstellungen des Administrationsagenten aktiviert ist.

Die Verbindungseinstellungen des Administrationsagenten mit dem Administrationsserver werden im Verbindungsprofil gespeichert. Im Verbindungsprofil können Sie Regeln für den Wechsel der Client-Geräte zu den Richtlinien für mobile Benutzer erstellen sowie das Profil so einrichten, dass es nur zum Download von Updatedateien verwendet wird.

Erstellen eines Verbindungsprofils für mobile Benutzer

Um für mobile Benutzer ein Profil für die Verbindung des Administrationsagenten zum Administrationsserver zu erstellen, gehen Sie wie folgt vor:

1. Wenn Sie ein Verbindungsprofil für eine Gruppe verwalteter Geräte erstellen möchten, öffnen Sie die Richtlinie des Administrationsagenten dieser Gruppe. Gehen Sie dafür folgendermaßen vor:

   a. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Richtlinien**.

   b. Wählen Sie die Administrationsgruppe aus, für die das Verbindungsprofil erstellt werden soll:

      - Für die Stammgruppe können Sie mit dem nächsten Schritt fortfahren.

      - Klicken Sie für eine Untergruppe im oberen Bereich der Seite auf die Schaltfläche **Hierarchie anzeigen** und anschließend im neuen Fenster auf den Namen der erforderlichen Untergruppe.

      Der Pfad zur ausgewählten Gruppe wird im oben Bereich der Seite angezeigt. Bei Bedarf können Sie auf einen Link mit dem Namen der Administrationsgruppe klicken, um zu dieser Gruppe zu gelangen. Der letzte Link im Pfad ist standardmäßig inaktiv. Außerdem können Sie das Hierarchiefenster schließen, indem Sie auf die Schaltfläche **Hierarchie verbergen** klicken.

   c. Fügen Sie die Richtlinie des Administrationsagenten für die Gruppe der verwalteten Geräte hinzu. Wenn Sie diese bereits erstellt haben, klicken Sie auf den Namen der Richtlinie des Administrationsagenten, um ihre Eigenschaften zu öffnen.

2. Wenn Sie ein Verbindungsprofil für ein bestimmtes verwaltetes Gerät erstellen möchten, gehen Sie wie folgt vor:

   a. Wechseln Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.

   b. Klicken Sie auf den Namen des verwalteten Geräts.

   c. Wechseln Sie im sich öffnenden Eigenschaftenfenster des verwalteten Geräts auf die Registerkarte **Anwendungen**.

   d. Klicken Sie auf den Namen der Richtlinie des Administrationsagenten, für die nur das ausgewählte verwaltete Gerät gilt.

3. Wechseln Sie im sich öffnenden Eigenschaftenfenster zu **Anwendungseinstellungen** → **Konnektivität** → **Verbindungsprofile.**

4. Klicken Sie im Abschnitt **Verbindungsprofile des Administrationsservers** auf **Hinzufügen**.

   Standardmäßig enthält die Liste der Verbindungsprofile die Profile <Autonomer-Modus> und <Home-Administrationsserver>. Diese Profile können nicht geändert oder gelöscht werden.

   Im Profil <Autonomer-Modus> ist kein Server für die Verbindung angegeben. Daher versucht der Administrationsagent beim Umschalten auf dieses Profil nicht, eine Verbindung zu einem Administrationsserver herzustellen, während auf Client-Geräten installierte Programme unter Mobilen Richtlinien ausgeführt werden. Das Profil <Autonomer-Modus> wird übernommen, wenn die Geräte vom Netzwerk getrennt sind.

   Das Profil <Home-Administrationsserver> gibt die Verbindung für den Administrationsserver an, der bei der Installation des Administrationsagenten festgelegt ausgewählt wurde. Das Profil <Home-Administrationsserver> wird verwendet, wenn ein Gerät in einem anderen Netzwerk erneut eine Verbindung zum Home-Administrationsserver herstellt.

5. Passen Sie im folgenden Fenster **Profil konfigurieren** die Einstellungen des Verbindungsprofils an:

   - **Profilname**

     In diesem Eingabefeld können Sie sich den Namen des Verbindungsprofils anzeigen lassen oder ihn ändern.

   - **Adresse des Administrationsservers**

     Adresse des Administrationsservers, zu dem das Client-Gerät eine Verbindung bei der Aktivierung des Profils herstellen soll.

   - **Port**

     Nummer des Ports, über den die Verbindung erfolgt.

   - **SSL-Port**

     Nummer des Ports, wenn die Verbindung mit dem SSL-Protokoll erfolgt.

   - **SSL-Verbindung verwenden**

     Wenn Sie die Option aktivieren, erfolgt die Verbindung über einen gesicherten Port (mit SSL-Protokoll).

     Diese Option ist standardmäßig aktiviert. Wir empfehlen, diese Option nicht zu deaktivieren, damit Ihre Verbindung gesichert bleibt.

- Aktivieren Sie die Option **Proxyserver verwenden**, wenn Sie einen Proxyserver für die Internetverbindung benutzen wollen. Wenn die Option aktiviert ist, sind Eingabefelder der Einstellungen verfügbar. Passen Sie die folgenden Verbindungseinstellungen für den Proxyserver an:

  - **Adresse**

    Die Proxyserver-Adresse für die Verbindung von Kaspersky Security Center Linux mit dem Internet.

  - **Port**

    Nummer des Ports, über den die Proxy-Verbindung zu Kaspersky Security Center Linux hergestellt wird.

  - **Authentifizierung am Proxyserver**

    Wenn das Kästchen aktiviert ist, können Sie in den Eingabefeldern Ihre Benutzerdaten zur Authentifizierung am Proxyserver angeben.

  - **Benutzername**

    Benutzerkonto, unter dem die Verbindung zum Proxyserver hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

  - **Kennwort**

    Kennwort, das von dem Benutzer festgelegt wird, unter dessen Benutzerkonto die Proxyserver-Verbindung hergestellt wird (dieses Feld ist verfügbar, wenn das Kontrollkästchen **Authentifizierung am Proxyserver** aktiviert ist).

    Um das eingegebene Kennwort anzuzeigen, klicken Sie auf die Schaltfläche **Anzeigen** und halten Sie diese für die erforderliche Zeitspanne gedrückt.

- **Adresse des Verbindungs-Gateways**

  Gateway-Adresse, über die Client-Geräte mit dem Administrationsserver verbunden werden.

- **Modus für mobile Benutzer aktivieren, wenn der Administrationsserver nicht verfügbar ist**

  Aktivieren Sie dieses Kontrollkästchen, damit bei der Verbindung von Programmen, die auf dem Client-Gerät installiert sind, Richtlinienprofile für Geräte, die sich im Modus für mobile Benutzer befinden, verwendet werden und die mobile Richtlinie verwendet wird, wenn der Administrationsserver nicht verfügbar ist. Wurde für das Programm keine Richtlinie für mobile Benutzer definiert, verwendet das Programm die aktive Richtlinie.

  Wenn diese Option deaktiviert ist, wenden die Anwendungen die aktiven Richtlinien an.

  Dieses Kontrollkästchen ist standardmäßig nicht aktiviert.

- **Nur für Update-Download verwenden**

  Wenn diese Option aktiviert ist, wird das Profil nur beim Update-Download von den auf dem Client-Gerät installierten Programmen verwendet. Bei den übrigen Vorgängen erfolgt eine Verbindung mit dem Administrationsserver mit den ursprünglichen Verbindungseinstellungen, die bei der Installation des Administrationsagenten eingegeben wurden.

  Diese Option ist standardmäßig aktiviert.

- **Verbindungseinstellungen mit den Einstellungen für den Administrationsserver synchronisieren, die in diesem Profil angegeben sind**

  Wenn diese Option aktiviert ist, stellt der Administrationsagent eine Verbindung zum Administrationsserver her und verwendet dazu die Einstellungen, die in den Profileigenschaften angegeben sind.

Wenn diese Option deaktiviert ist, stellt der Administrationsagent eine Verbindung zum Administrationsserver mithilfe der bei der Installation angegebenen ursprünglichen Einstellungen her.

Diese Option ist verfügbar, wenn die Option **Nur für Update-Download verwenden** aktiviert ist.

Diese Option ist standardmäßig deaktiviert.

Für mobiler Benutzer wird ein Profil zur Verbindung des Administrationsagenten zum Administrationsserver erstellt. Wird mit diesem Profil eine Verbindung des Administrationsagenten zum Administrationsserver hergestellt, so verwenden die auf dem Client-Gerät installierten Programme Richtlinien für Geräte, die sich im Modus für mobile Benutzer befinden, oder mobile Richtlinien.

Remote-Zugriff auf verwaltete Geräte

Dieser Abschnitt enthält Informationen über den Remote-Zugriff auf verwaltete Geräte.

Verwenden der Option "Verbindung mit Administrationsserver nicht trennen" zur Bereitstellung einer dauerhaften Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver

Wenn Sie keine Push-Server verwenden, bietet Kaspersky Security Center Linux keine kontinuierliche Verbindung zwischen verwalteten Geräten und dem Administrationsserver. Die Administrationsagenten auf den verwalteten Geräten stellen regelmäßig eine Verbindung mit dem Administrationsserver her und führen eine Synchronisierung durch. Die Dauer des Zeitraums einer solcher Synchronisierung wird in der Richtlinie des Administrationsagenten festgelegt. Wenn eine frühzeitige Synchronisierung erforderlich ist, sendet der Administrationsserver (oder ein Verteilungspunkt, falls verwendetet) ein signiertes Netzwerkpaket über ein IPv4- oder IPv6-Netzwerk an den UDP-Port des Administrationsagenten. Standardmäßig wird Port 15000 verwendet. Wenn über UDP keine Verbindung vom Administrationsserver zum verwalteten Gerät möglich ist, wird die Synchronisierung bei der nächsten routinemäßigen Verbindung des Administrationsagenten mit dem Administrationsserver im Laufe des Synchronisierungsintervalls durchgeführt.

Einige Vorgänge können ohne eine frühzeitige Verbindung zwischen dem Administrationsagenten und dem Administrationsserver nicht ausgeführt werden, wie z. B. das Starten und Stoppen lokaler Aufgaben oder das Empfangen von Statistiken für ein verwaltetes Programm. Um dieses Problem für den Fall zu beheben, dass Sie keine Push-Server verwenden, können Sie die Option **Verbindung mit Administrationsserver nicht trennen** verwenden, um sicherzustellen, dass eine kontinuierliche Verbindung zwischen einem verwalteten Gerät und dem Administrationsserver besteht.

So stellen Sie eine dauerhafte Verbindung zwischen einem Client-Gerät und dem Administrationsserver bereit:

1. Gehen Sie im Hauptmenü zu **Asset-Verwaltung** → **Assets (Geräte)**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Klicken Sie in der Liste der verwalteten Geräte auf den Link mit dem Namen des entsprechenden Geräts.

3. Aktivieren Sie im Eigenschaftsfenster im Abschnitt **Allgemein** die Option **Verbindung mit Administrationsserver nicht trennen**.

Zwischen dem verwalteten Gerät und Administrationsserver wurde eine dauerhafte Verbindung hergestellt.

Die maximale Gesamtzahl der Geräte mit ausgewählter Option **Verbindung mit Administrationsserver nicht trennen** beträgt 300.

Über das Überprüfen der Verbindungszeit des Geräts mit dem Administrationsserver

Wenn ein Gerät heruntergefahren wird, benachrichtigt der Administrationsagent den Administrationsserver über dieses Ereignis. In der Kaspersky Security Center Web Console wird das Gerät als heruntergefahren angezeigt. Der Administrationsagent kann den Administrationsserver jedoch nicht über alle derartigen Ereignisse benachrichtigen. Der Administrationsserver analysiert deshalb periodisch das Attribut **Verbindung mit dem Administrationsserver** (Der Wert dieses Attributs wird in der Kaspersky Security Center Web Console in den Geräteeigenschaften im Abschnitt **Allgemein** angezeigt) für jedes Gerät und vergleicht es mit dem Synchronisierungsintervall aus den aktuellen Einstellungen des Administrationsagenten. Wenn ein Gerät über mehr als drei aufeinander folgende Synchronisationsintervalle nicht reagiert hat, wird dieses Gerät als abgeschaltet markiert.

Über erzwungene Synchronisierung

Obwohl Kaspersky Security Center Linux den Status, die Einstellungen, die Aufgaben und die Richtlinien für die verwalteten Geräte automatisch synchronisiert, muss der Administrator in einzelnen Fällen genau wissen, ob an diesem Moment für ein bestimmtes Gerät die Synchronisierung ausgeführt worden ist.

Im Eigenschaftsfenster eines verwalteten Geräts befindet sich die Schaltfläche **Synchronisierung erzwingen**. Wenn Kaspersky Security Center Linux den Befehl zur Synchronisierung ausführt, versucht der Administrationsserver, eine Verbindung zum Gerät herzustellen. Ist dieser Versuch erfolgreich, so wird die Synchronisierung erzwungen. Andernfalls erfolgt die erzwungene Synchronisierung erst nach der nächsten geplanten Verbindung des Administrationsagenten mit dem Administrationsserver.

Handbuch zur Skalierung

Dieser Abschnitt enthält Informationen über die Skalierung von Kaspersky Security Center Linux.

Zu diesem Handbuch

Das Handbuch zur Skalierung von Kaspersky Security Center Linux (auch als "Kaspersky Security Center" bezeichnet) richtet sich an Experten, die für die Installation und Administration von Kaspersky Security Center zuständig sind, sowie an Experten, die für den technischen Support von Unternehmen verantwortlich sind, die Kaspersky Security Center einsetzen.

Alle Empfehlungen und Berechnungen sind für Netzwerke vorgesehen, in denen Kaspersky Security Center den Schutz von Geräten mit installierter Software von Kaspersky verwaltet.

Zur Erreichung und Aufrechterhaltung der optimalen Leistung unter verschiedenen Arbeitsbedingungen berücksichtigen Sie die Anzahl der Geräte im Netzwerk, die Netztopologie und den erforderlichen Funktionsumfang von Kaspersky Security Center.

Das Handbuch enthält folgende Informationen:

- Einschränkungen von Kaspersky Security Center
- Berechnungen für die wichtigsten Nodes von Kaspersky Security Center (Administrationsserver und Verteilungspunkte):
    - Hardwarevoraussetzungen für die Administrationsserver und Verteilungspunkte
    - Berechnung der Anzahl und der Hierarchie der Administrationsserver
    - Berechnung der Anzahl und der Konfiguration der Verteilungspunkte
- Konfiguration der Speicherung von Ereignissen in der Datenbank in Abhängigkeit von der Anzahl der Geräte im Netzwerk
- Bewährte Methoden zur Optimierung der Leistungs
- Konfiguration bestimmter Aufgaben, welche die optimale Leistung von Kaspersky Security Center gewährleisten
- Verbrauch von Datenverkehr (Netzwerkbelastung) zwischen dem Kaspersky Security Center Administrationsserver und jedem geschützten Gerät

Es wird empfohlen, dieses Handbuch in den folgenden Situationen zu konsultieren:

- Wenn Sie vor der Installation von Kaspersky Security Center die Verteilung von Ressourcen planen.
- Wenn Sie die Größe des Netzwerks wesentlich ändern möchten, in dem Kaspersky Security Center bereitgestellt wurde.

- Wenn Sie Kaspersky Security Center bisher innerhalb eines begrenzten Netzwerksegments (in einer Testumgebung) verwendet haben und jetzt zur vollständigen Bereitstellung von Kaspersky Security Center im Unternehmensnetzwerk wechseln.

- Bei Änderungen in der Auswahl der verwendeten Funktionen von Kaspersky Security Center.

Berechnungen für die Administrationsserver

Dieser Abschnitt enthält die Software- und Hardwareanforderungen für Geräte, die als Administrationsserver verwendet werden. Ferner werden Empfehlungen für die Berechnung der Anzahl und für die Hierarchie von Administrationsservern abhängig von der Konfiguration des Unternehmensnetzwerks bereitgestellt.

Es wird empfohlen, nach der Installation des Administrationsservers und des DBMS auf diesen Geräten ebenfalls Kaspersky Endpoint Security für Linux zu installieren. Weitere Informationen zu den Hardware-Anforderungen von Kaspersky Endpoint Security finden Sie in der Hilfe zu Kaspersky Endpoint Security für Linux.

Die Last, die Kaspersky Endpoint Security für Linux bei einer Integration mit Managed Detection and Response und lokalem Kaspersky Endpoint Detection and Response Expert erzeugt, wird bei der Berechnung für die gleichzeitige Installation von Kaspersky Security Center Linux und KES_LIN nicht berücksichtigt.

Berechnung von Hardwareressourcen für den Administrationsserver

Dieser Abschnitt enthält Berechnungen, die bei der Planung der Hardwareressourcen für den Administrationsserver verwendet werden können.

Hardwarevoraussetzungen für DBMS und Administrationsserver

Die nachfolgenden Tabellen zeigen die empfohlenen, anhand eines Tests ermittelten, minimalen Hardwarevoraussetzungen für das DBMS und den Administrationsserver. Die vollständige Liste mit unterstützten Betriebssystemen und DBMS finden Sie bei den Hard- und Softwarevoraussetzungen.

> Auf dem Gerät mit dem installierten Administrationsserver müssen Sie die Verwendung der Swap-Datei aktivieren. Die Swap-Datei muss mindestens 1.5-mal größer sein als der Arbeitsspeicher.

Es wird empfohlen, nach der Installation des Administrationsservers und des DBMS auf diesen Geräten ebenfalls Kaspersky Endpoint Security für Linux zu installieren.
Für die gleichzeitige Installation sind mindestens 225 IOPS erforderlich. Zusätzlich erhöhen sich die Anforderungen an den Administrationsserver mit DBMS um 1,5 GB RAM
. Die Hardwarevoraussetzungen für Kaspersky Endpoint Security finden Sie in der Hilfe zu Kaspersky Endpoint Security für Linux.

Das Netzwerk umfasst 50,000 Geräte

Konfiguration des Geräts mit dem Administrationsserver

Hardware	Wert
Prozessor	8 Kerne (12 Kerne empfohlen), 2500 MHz
Arbeitsspeicher	16 GB
Speicherplatz	300 GB, 150 IOPS oder höher

Konfiguration eines Geräts mit installiertem PostgreSQL DBMS

Hardware	Wert
Prozessor	16 Kerne, 2500 MHz
Arbeitsspeicher	32 GB
Speicherplatz	300 GB, 150 IOPS oder höher

Konfiguration von Knoten für einen Failover-Cluster

Hardware	Wert
Prozessor	16 Kerne, 2500 MHz
Arbeitsspeicher	32 GB
Speicherplatz	500 GB, 300 IOPS oder höher
Netzwerkschnittstellen-Controller	1 Gbit/s

Konfiguration des Geräts auf dem sowohl der Administrationsserver und als auch das DBMS PostgreSQL installiert ist.

Hardware	Wert
Prozessor	24 Kerne (28 Kerne empfohlen), 2500 MHz
Arbeitsspeicher	48 GB
Speicherplatz	600 GB, 300 IOPS oder höher

Das Netzwerk umfasst 30,000 Geräte

Konfiguration des Geräts mit dem Administrationsserver

Hardware	Wert
Prozessor	6 Kerne (8 Kerne empfohlen), 2500 MHz
Arbeitsspeicher	12 GB
Speicherplatz	200 GB, 150 IOPS oder höher

Konfiguration eines Geräts mit installiertem PostgreSQL DBMS

Hardware	Wert
Prozessor	12 Kerne, 2500 MHz
Arbeitsspeicher	22 GB
Speicherplatz	250 GB, 150 IOPS oder höher

Konfiguration von Knoten für einen Failover-Cluster

Hardware	Wert
Prozessor	16 Kerne, 2500 MHz
Arbeitsspeicher	32 GB
Speicherplatz	500 GB, 300 IOPS oder höher
Netzwerkschnittstellen-Controller	1 Gbit/s

Konfiguration des Geräts auf dem sowohl der Administrationsserver und als auch das DBMS PostgreSQL installiert ist.

Hardware	Wert
Prozessor	16 Kerne (20 Kerne empfohlen), 2500 MHz
Arbeitsspeicher	34 GB
Speicherplatz	450 GB, 300 IOPS oder höher

Das Netzwerk umfasst 10,000 Geräte

Konfiguration des Geräts mit dem Administrationsserver

Hardware	Wert
Prozessor	4 Kerne (6 Kerne empfohlen), 2500 MHz
Arbeitsspeicher	8 GB
Speicherplatz	100 GB, 150 IOPS oder höher

Konfiguration eines Geräts mit installiertem PostgreSQL DBMS

Hardware	Wert
Prozessor	6 Kerne, 2500 MHz
Arbeitsspeicher	10 GB
Speicherplatz	200 GB, 150 IOPS oder höher

Konfiguration von Knoten für einen Failover-Cluster

Hardware	Wert
Prozessor	16 Kerne, 2500 MHz
Arbeitsspeicher	32 GB
Speicherplatz	500 GB, 300 IOPS oder höher
Netzwerkschnittstellen-Controller	1 Gbit/s

Konfiguration des Geräts auf dem sowohl der Administrationsserver und als auch das DBMS PostgreSQL installiert ist.

Hardware	Wert
Prozessor	8 Kerne (14 Kerne empfohlen), 2500 MHz
Arbeitsspeicher	18 GB
Speicherplatz	300 GB, 300 IOPS oder höher

Das Netzwerk umfasst 1000 Geräte

Konfiguration des Geräts mit dem Administrationsserver

Hardware	Wert
Prozessor	2 Kerne, 2500 MHz
Arbeitsspeicher	6 GB
Speicherplatz	10 GB, 150 IOPS oder höher

Konfiguration eines Geräts mit installiertem PostgreSQL DBMS

Hardware	Wert
Prozessor	2 Kerne, 2500 MHz
Arbeitsspeicher	4 GB
Speicherplatz	20 GB, 150 IOPS oder höher

Konfiguration von Knoten für einen Failover-Cluster

Hardware	Wert
Prozessor	16 Kerne, 2500 MHz
Arbeitsspeicher	32 GB
Speicherplatz	500 GB, 300 IOPS oder höher
Netzwerkschnittstellen-Controller	1 Gbit/s

Konfiguration des Geräts auf dem sowohl der Administrationsserver und als auch das DBMS PostgreSQL installiert ist.

Hardware	Wert
Prozessor	4 Kerne, 2500 MHz
Arbeitsspeicher	10 GB
Speicherplatz	30 GB, 300 IOPS oder höher

Die Tests wurden mit den folgenden Einstellungen durchgeführt:

- Auf dem Administrationsserver ist die automatische Bestimmung von Verteilungspunkten aktiviert oder die Verteilungspunkte werden manuell gemäß der empfohlenen Tabelle bestimmt
- Das PostgreSQL-DBMS enthält keine anderen Erweiterungen als plpgsql.

Auf dem Gerät, auf dem DBMS installiert ist, belegt die Datenbank ungefähr 100 GB an Speicherplatz und das Protokoll der Transaktionen ungefähr 200 GB.

Berechnung des Speicherplatzes in der Datenbank

Der Speicherplatz, der von der Datenbank belegt wird, kann näherungsweise mit folgender Formel berechnet werden:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

wobei:

- "C" – Anzahl der Geräte.
- "E" – Anzahl der gespeicherten Ereignisse.
- "A" – Gesamtsumme der Active Directory-Objekte:
  - Benutzerkonten der Geräte
  - Benutzerkonten
  - Benutzerkonten der Sicherheitsgruppen
  - Unterverzeichnisse von Active Directory

  Wenn die Abfrage von Active Directory deaktiviert ist, dann muss der Wert "A" mit Null angenommen werden.
- N ist die durchschnittliche Anzahl inventarisierter ausführbarer Dateien auf einem Endpunktgerät.
- F ist die Anzahl der Endpunktegeräte, auf denen ausführbare Dateien inventarisiert wurden.

Wenn Sie in den Einstellungen der Richtlinie für Kaspersky Endpoint Security die Übermittlung von Informationen über die ausgeführten Programme an den Administrationsserver aktivieren möchten, werden für die Speicherung der Informationen über die ausgeführten Programme weitere (0,03 * C) GB benötigt.

Während der Ausführung bildet sich in der Datenbank immer ein sogenannter *nicht benutzter Speicherplatz* (unallocated space). Aus diesem Grund ist die tatsächliche Größe der Datenbankdatei in der Regel ungefähr doppelt so groß wie der Speicherplatz in der Datenbank.

Es wird nicht empfohlen, die Größe des Transportprotokolls explizit zu begrenzen. Behalten Sie den Standardwert des Parameters MAXSIZE bei.

Berechnung des benötigten Speicherplatzes auf der Festplatte

Der vom Verzeichnis "/var/opt/kaspersky/klnagent_srv/" benötigte Speicherplatz auf dem Laufwerk des Administrationsservers kann anhand folgender Formel annähernd berechnet werden:

(724 * C + 0,15 * E + 0,17 * A), KB

wobei:

- "C" – Anzahl der Geräte.
- "E" – Anzahl der gespeicherten Ereignisse.
- "A" – Gesamtsumme der Active Directory-Objekte:
  - Benutzerkonten der Geräte
  - Benutzerkonten
  - Benutzerkonten der Sicherheitsgruppen
  - Unterverzeichnisse von Active Directory

Wenn die Abfrage von Active Directory deaktiviert ist, dann muss der Wert "A" mit Null angenommen werden.

Berechnung der Anzahl und der Konfiguration der Administrationsserver

Um die Auslastung des primären Administrationsservers zu verringern, können Sie jeder Administrationsgruppe einen separaten Administrationsserver zuweisen. Die Anzahl der sekundären Administrationsserver eines primären Administrationsservers darf höchstens 500 betragen.

Es wird empfohlen, bei der Konfiguration der Administrationsserver die Struktur Ihres Unternehmensnetzwerks zu berücksichtigen.

Empfehlungen für die Verbindung dynamischer virtueller Maschinen mit Kaspersky Security Center

Dynamische virtuelle Maschinen (auch als dynamische VMs bezeichnet) verbrauchen mehr Ressourcen als statische virtuelle Maschinen.

Weitere Informationen zu dynamischen virtuellen Maschinen finden Sie unter Unterstützung dynamischer virtueller Maschinen.

Wenn eine neue dynamische VM verbunden wird, erstellt Kaspersky Security Center Linux einen Eintrag für diese dynamische VM in der Kaspersky Security Center Web Console und verschiebt die dynamische VM in die Administrationsgruppe. Anschließend wird die dynamische VM zur Administrationsserver-Datenbank hinzugefügt. Der Administrationsserver wird vollständig mit dem Administrationsagenten synchronisiert, der auf dieser dynamischen VM installiert ist.

Im Netzwerk einer Organisation erstellt der Administrationsagent die folgenden Netzwerklisten für jede dynamische VM:

- Hardware
- Installierte Software
- Erkannte Schwachstellen
- Ereignisse und Listen von ausführbaren Dateien der Komponente "Programmkontrolle"

Der Administrationsagent überträgt diese Netzwerklisten an den Administrationsserver. Die Größe der Netzwerklisten hängt von den auf der dynamischen VM installierten Komponenten ab und kann die Leistung von Kaspersky Security Center Linux und Datenbankverwaltungssystems (DBMS) beeinträchtigen. Beachten Sie, dass die Belastung nichtlinear wachsen kann.

Nachdem der Benutzer die Arbeit mit der dynamischen VM beendet und sie ausgeschaltet hat, wird diese Maschine aus der virtuellen Infrastruktur entfernt und Einträge zu dieser Maschine werden aus der Administrationsserver-Datenbank entfernt.

All diese Aktionen verbrauchen viele Datenbankressourcen von Kaspersky Security Center Linux und dem Administrationsserver und können die Leistung von Kaspersky Security Center Linux und des DBMS beeinträchtigen. Wir empfehlen, dass Sie bis zu 20.000 dynamische VMs mit Kaspersky Security Center Linux zu verbinden.

Sie können mehr als 20.000 dynamische VMs mit Kaspersky Security Center Linux verbinden, wenn die verbundenen dynamischen VMs Standardvorgänge ausführen (z. B. Datenbankaktualisierungen) und nicht mehr als 80% des Arbeitsspeichers und 75–80% der verfügbaren Kerne verbrauchen.

Das Ändern von Richtlinieneinstellungen, Programmen oder Betriebssystemen auf den dynamischen VMs kann den Ressourcenverbrauch verringern oder erhöhen. Als optimal gilt ein Verbrauch von 80–95% der Ressourcen.

Berechnungen für Verteilungspunkte und Verbindungs-Gateways

Dieser Abschnitt enthält die Hardwarevoraussetzungen für die Geräte, die als Verteilungspunkte verwendet werden, sowie Empfehlungen zur Berechnung der Anzahl von Verteilungspunkten und Verbindungs-Gateways in Abhängigkeit von der Struktur des Unternehmensnetzwerks.

Anforderungen an einen Verteilungspunkt

In diesem Artikel werden die Hardware- und Softwareanforderungen für Windows- und Linux-basierte Verteilungspunkte beschrieben.

Wenn auf dem Administrationsserver Aufgaben zur Remote-Installation vorhanden sind, ist auf dem Gerät mit dem Verteilungspunkt zusätzlicher Speicherplatz in der Größe erforderlich, die der Summe aller zu installierenden Installationspakete entspricht.

Wenn auf dem Administrationsserver ein oder mehrere Instanzen einer Aufgabe zur Installation von Updates (Patches) und zum Schließen von Schwachstellen vorhanden sind, ist auf dem Gerät mit dem Verteilungspunkt zusätzlicher Speicherplatz in der Größe erforderlich, die der doppelten Summe aller zu installierenden Patches erforderlich.

Bei Verwendung des Schemas, bei dem die Verteilungspunkte die Datenbanken-Updates und Programm-Module direkt von den Kaspersky-Update-Servern abrufen, müssen die Verteilungspunkte mit dem Internet verbunden sein.

> Es wird nicht empfohlen, den Administrationsserver als Verteilungspunkt zuzuweisen, da dies die Belastung des Administrationsservers erhöht.

Hardwareanforderungen für Windows-basierte Verteilungspunkte

Minimale Hardwareanforderungen für Windows-basierte Verteilungspunkte

Anzahl an Client-Geräten	Prozessor	Arbeitsspeicher	Arbeitsspeicher, mit aktiviertem Patch-Management	Speicherplatz
10.000	4 Kerne, 2500 MHz	8 GB	8 GB	120 GB
5 000	4 Kerne, 2500 MHz	6 GB	8 GB	120 GB
1.000	2 Kerne, 2500 MHz	4 GB	8 GB	120 GB

Hardwareanforderungen für Linux-basierte Verteilungspunkte

Minimale Hardwareanforderungen für Linux-basierte Verteilungspunkte

Anzahl an Client-Geräten	Prozessor	Arbeitsspeicher	Speicherplatz
10.000	4 Kerne, 2500 MHz	10 GB	120 GB
5 000	4 Kerne, 2500 MHz	8 GB	120 GB
1.000	2 Kerne, 2500 MHz	6 GB	120 GB

Anzahl und Konfiguration der Verteilungspunkte bestimmen

Je mehr Client-Geräte ein Netzwerk enthält, desto mehr Verteilungspunkte sind erforderlich. Es wird empfohlen, die automatische Zuweisung von Verteilungspunkten nicht zu deaktivieren. Bei aktivierter automatischer Zuweisung der Verteilungspunkte weist der Administrationsserver bei einer großen Anzahl an Client-Geräten automatisch Verteilungspunkte zu und bestimmt ihre Konfiguration.

Verwendung exklusiv zugewiesener Verteilungspunkte

Wenn Sie planen, als Verteilungspunkte eine Reihe von bestimmten Geräten zu verwenden (d. h., exklusiv zugewiesene Server), so können Sie auf die automatische Zuweisung der Verteilungspunkte verzichten. Überzeugen Sie sich in diesem Fall davon, dass die Geräte, die Sie zu Verteilungspunkten bestimmen möchten, über ausreichend freien Speicherplatz auf dem Datenträger verfügen, nicht regelmäßig abgeschaltet werden und dass auf ihnen der Ruhezustand deaktiviert ist.

Anzahl der exklusiv zugewiesenen Verteilungspunkte in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, ein einzelnes Netzwerksegment enthält

Anzahl der Client-Geräte in dem Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 300	0 (Es müssen keine Verteilungspunkte bestimmt werden)
Über 300	Akzeptabel: (N/10.000 +1), empfohlen: (N/5000+2), wobei N die Anzahl an Geräten im Netzwerk ist

Anzahl der exklusiv zugewiesenen Verteilungspunkte in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, mehrere Netzwerksegmente enthält

Anzahl der Client-Geräte pro Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 10	0 (Es müssen keine Verteilungspunkte bestimmt werden)
10–100	1
Über 100	Akzeptabel: (N/10.000 +1), empfohlen: (N/5000+2), wobei N die Anzahl an Geräten im Netzwerk ist

Verwendung von Standard-Client-Geräten (Workstations) als Verteilungspunkte

Wenn Sie planen, als Verteilungspunkte Standard-Client-Geräte (d. h., Workstations) zu verwenden, wird zur Vermeidung einer unnötigen Belastung des Administrationsservers empfohlen, die Verteilungspunkte auf folgende Weise zuzuweisen (s. nachfolgende Tabelle):

Anzahl der als Verteilungspunkte fungierenden Workstations in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, ein einzelnes Netzwerksegment enthält

Anzahl der Client-Geräte in dem Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 300	0 (Es müssen keine Verteilungspunkte bestimmt werden)
Über 300	(N/300 +1), wobei N die Anzahl an Geräten im Netzwerk ist, jedoch mindestens 3 Verteilungspunkte

Anzahl der als Verteilungspunkte fungierenden Workstations in einem Netzwerk, das, basierend auf der Anzahl der Netzwerkgeräte, mehrere Netzwerksegmente enthält

Anzahl der Client-Geräte pro Netzwerksegment	Anzahl der Verteilungspunkte
Weniger als 10	0 (Es müssen keine Verteilungspunkte bestimmt werden)
10–30	1
31–300	2
Über 300	(N/300 +1), wobei N die Anzahl an Geräten im Netzwerk ist, jedoch mindestens 3 Verteilungspunkte

Wenn ein Verteilungspunkt abgeschaltet (oder aus anderen Gründen nicht verfügbar) ist, können die verwalteten Geräte in seinem Bereich Updates vom Administrationsserver abrufen.

Berechnung der Anzahl der Verbindungs-Gateways

Wenn Sie ein Verbindungs-Gateway verwenden möchten, wird empfohlen, ein Gerät speziell für diesen Zweck zu bestimmen.

Ein Verbindungs-Gateway kann maximal 10.000 verwaltete Geräte abdecken.

Speicherung der Daten zu Ereignissen für Aufgaben und Richtlinien

Dieser Abschnitt enthält Berechnungen, die sich auf die Speicherung von Ereignissen in der Administrationsserver-Datenbank beziehen, sowie Empfehlungen zur Minimierung der Anzahl der Ereignisse und der Reduzierung der Auslastung des Administrationsservers.

Standardmäßig ist in den Eigenschaften jeder Aufgabe und Richtlinie die Protokollierung aller Ereignisse aktiviert, die mit der Aufgabenausführung und der Anwendung der Richtlinie verbunden sind.

Wenn jedoch eine Aufgabe recht häufig (z. B. mehr als einmal pro Woche) auf einer recht großen Anzahl an Geräten (z. B. auf mehr als 10.000) ausgeführt wird, kann sich eine große Anzahl an Ereignissen ansammeln, welche die Datenbank überfüllen. In einem solchen Fall wird empfohlen, in den Eigenschaften der Aufgabe eine von zwei anderen Optionen festzulegen:

- **Ereignisse in Bezug auf den Aufgabenfortschritt speichern**. In diesem Fall gehen von jedem Gerät, auf dem die Aufgabe ausgeführt wird, nur Informationen über den Start, den Verlauf und den Abschluss der Aufgabe (erfolgreich, mit Warnung oder mit einem Fehler) in die Datenbank ein.

- **Nur die Ergebnisse der Aufgabenausführung speichern**. In diesem Fall gehen von jedem Gerät, auf dem die Aufgabe ausgeführt wird, nur Informationen über den Abschluss der Aufgabe (erfolgreich, mit Warnung oder mit einem Fehler) in die Datenbank ein.

Wenn eine Richtlinie einer recht großen Anzahl an Geräten zugewiesen ist (z. B. mehr als 10.000), kann sich eine große Anzahl an Ereignissen ansammeln, welche die Datenbank überfüllen. In einem solchen Fall wird empfohlen, in den Eigenschaften der Richtlinie nur die kritischen Ereignisse auszuwählen und ihre Speicherung zu aktivieren. Es wird empfohlen, die Speicherung aller anderen Ereignisse zu deaktivieren.

Auf diese Weise reduzieren Sie die Anzahl der Ereignisse in der Datenbank, erhöhen die Ausführungsgeschwindigkeit der Szenarien, die mit der Analyse der Ereignistabelle in der Datenbank verbunden sind, und reduzieren das Risiko der Verdrängung von kritischen Ereignissen durch eine große Anzahl an Ereignissen.

Sie können außerdem die Aufbewahrungsdauer der Ereignisse reduzieren, die mit der Aufgabe (Richtlinie) verbunden sind. Standardmäßig beträgt diese Frist 7 Tage für Ereignisse, die mit einer Aufgabe verbunden sind, und 30 Tage für Ereignisse, die mit einer Richtlinie verbunden sind. Beachten Sie bei der Änderung der Aufbewahrungsfrist der Ereignisse die üblichen Arbeitsvorgänge in Ihrem Unternehmen und die Zeit, die dem Systemadministrator zur Analyse jedes Ereignisses zur Verfügung steht.

In jedem der folgenden Fälle ist es sinnvoll, die Speicherung der Ereignisse zu bearbeiten:

- Ereignisse über die Änderung von temporären Statusvarianten der Gruppenaufgaben und Ereignisse über die Anwendung von Richtlinien stellen einen wesentlichen Anteil aller Ereignisse in der Datenbank von Kaspersky Security Center Linux dar.

- Im Betriebssystem-Protokoll erscheinen Einträge zum automatischen Löschen von Ereignissen aufgrund der Überschreitung des festgelegten Grenzwertes für die Gesamtzahl der Ereignisse, die in der Datenbank gespeichert sind.

Beachten Sie bei der Auswahl der Ereignisprotokollierungs-Optionen, dass die optimale Anzahl der Ereignisse, die von einem einzelnen Gerät stammen, maximal 20 Ereignisse pro Tag beträgt. Sie können diese Beschränkung erforderlichenfalls leicht erhöhen, jedoch nur, wenn die Anzahl an Geräten in Ihrem Netzwerk relativ klein ist (weniger als 10.000).

Bewährte Methoden für einen Administrationsserver, der eine hohe Anzahl von Geräten verwaltet

Bewährte Methode zur Verwendung eines DBMS

Konfigurieren Sie die Aufgabe zur **Wartung des Administrationsservers** so, dass sie regelmäßig ausgeführt wird. Dies gilt insbesondere, wenn Sie PostgreSQL als DBMS verwenden.

Schließen Sie den Ordner des DBMS von der IOC-Untersuchung aus.

Bewährte Methoden für Richtlinien und Profile

Verringern Sie die Anzahl der aktiven Richtlinien für eine Komponente (z. B. Kaspersky Endpoint Security für Windows). Sie können Richtlinien durch Richtlinienprofile ersetzen.

Bewährte Verfahren für einen Administrationsserver, der eine hohe Anzahl von Geräten verwaltet

Reduzieren Sie die Anzahl der gleichzeitig ausgeführten Aufgaben, insbesondere Aufgaben zur Remote-Installation und zum Patch-Management.

Reduzieren Sie die Anzahl der Aufgaben, die Geräteauswahlen verwenden, und optimieren Sie den Zeitplan für solche Aufgaben.

Im Abschnitt **Konfiguration von Ereignissen** der Richtlinieneinstellungen können Sie die Anzahl der zu speichernden Ereignistypen verringern.

Bewährte Methoden zum Speichern von Ereignissen

Verringern Sie für die Programmkontrolle die Häufigkeit von Ereignissen einzelner Typen. Weitere Informationen finden Sie im Artikel Über das Blockieren von häufig auftretenden Ereignissen.

Verkürzen Sie die Speicherdauer für Ereignisse von Komponenten (z. B. Kaspersky Endpoint Security für Windows) und für informative Ereignisse über behobene Schwachstellen.

Aktivieren Sie die Option **Ereignisse in Bezug auf den Aufgabenfortschritt speichern** in den Einstellungen allgemeiner Aufgaben, z. B. Update-Aufgaben. Weitere Informationen finden Sie im Artikel Speicherung der Daten zu Ereignissen für Aufgaben und Richtlinien.

Optimieren Sie die Einstellungen der Inventarisierungsaufgabe. Weitere Informationen finden Sie im Artikel Inventarisierungsaufgabe.

Besonderheiten und optimale Einstellungen bestimmter Aufgaben

Einige Aufgaben verfügen über Besonderheiten, die mit der Anzahl der Geräte im Netzwerk zusammenhängen. In diesem Abschnitt finden Sie Empfehlungen für die optimale Konfiguration solcher Aufgaben.

Die Gerätesuche, die Aufgabe zum Anlegen eines Daten-Backups, die Aufgabe zur Pflege von Datenbanken sowie die Gruppenaufgaben zum Update von Kaspersky Endpoint Security gehören zum grundlegenden Funktionsumfang von Kaspersky Security Center Linux.

Die Aufgabe zur Inventarisierung gehört zur Funktionalität Schwachstellen- und Patch-Management und ist nicht verfügbar, wenn diese Funktionalität nicht aktiviert ist.

Häufigkeit der Gerätesuche

Es wird nicht empfohlen, die voreingestellte Häufigkeit der Gerätesuche zu erhöhen, da dies zu einer übermäßigen Belastung der Domänencontroller führen kann. Es wird vielmehr empfohlen, für den Zeitplan der Abfrage eine möglichst geringe Häufigkeit festzulegen, sofern die Konfiguration Ihres Unternehmens dies erlaubt. Die nachfolgende Tabelle enthält Empfehlungen für die Berechnung des optimalen Zeitplans.

Zeitplan der Gerätesuche

Anzahl der Geräte im Netzwerk	Empfohlene Häufigkeit der Gerätesuche
Weniger als 10.000	Wie voreingestellt oder seltener
10.000 und mehr	Einmal pro Tag oder seltener

Aufgaben zum Sichern der Daten des Administrationsservers und zur Pflege von Datenbanken

Der Administrationsserver stellt während der Ausführung folgender Aufgaben seine Funktion ein:

- Backup der Daten des Administrationsservers anlegen
- Wartung des Administrationsservers

Solange diese Aufgaben ausgeführt werden, können keine Daten in die Datenbank eingehen.

Eventuell müssen Sie den Zeitplan dieser Aufgaben so anpassen, dass ihre Ausführung sich nicht mit der Ausführung anderer Aufgaben des Administrationsservers überschneidet.

Gruppenaufgaben zum Update von Kaspersky Endpoint Security

Wenn der Administrationsserver als Update-Quelle dient, wird für Gruppenaufgaben zum Update von Kaspersky Endpoint Security Version 10 und höher der Zeitplan **Nach dem Download von Updates in die Datenverwaltung** mit aktiviertem Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** empfohlen.

Wenn Sie auf jedem Verteilungspunkt eine lokale Aufgabe für den Download von Updates von den Servern von Kaspersky in den Speicher erstellt haben, wird für die Gruppenaufgabe zum Update von Kaspersky Endpoint Security ein regelmäßiger Zeitplan empfohlen. In diesem Fall muss als Zeitraum für den zufälligen Start eine Stunde angegeben werden.

Inventarisierungsaufgabe

Sie können die Auslastung der Datenbank verringern und gleichzeitig Informationen über die ausführbaren Dateien erhalten. Dazu empfehlen wir, dass Sie eine Bestandsaufnahme für Kaspersky Endpoint Security auf den Referenzgeräten durchführen, auf denen ein Standardpaket von Software installiert ist.

Die Anzahl ausführbarer Dateien, die der Administrationsserver erhält, darf 150.000 nicht überschreiten. Wenn diese Grenze erreicht wird, erhält Kaspersky Security Center Linux keine neuen Dateien mehr.

Die Anzahl der Dateien auf einem gewöhnlichen verwalteten Client-Gerät beträgt in der Regel nicht mehr als 60.000. Die Anzahl der ausführbaren Dateien auf dem Dateiserver kann noch mehr betragen und sogar den Grenzwert von 150.000 überschreiten.

Informationen zur Netzwerkauslastung zwischen dem Administrationsserver und den geschützten Geräten

Dieser Abschnitt enthält die Ergebnisse der Testmessungen des Datenverkehrs im Netzwerk unter Angabe der Bedingungen, unter denen die Messungen vorgenommen wurden. Sie können diese Informationen als Richtwerte bei der Planung der Netzwerkinfrastruktur und der Bandbreite der Kanäle innerhalb des Unternehmens (oder zwischen dem Administrationsserver und dem Unternehmen, in dem sich die geschützten Geräte befinden) verwenden. Außerdem können Sie bei Kenntnis der Bandbreite des Netzwerks ungefähr einschätzen, wie viel Zeit bestimmte Datenübertragungsoperationen in Anspruch nehmen.

Verbrauch von Datenverkehr bei der Ausführung verschiedener Szenarien

Die nachfolgende Tabelle enthält die Ergebnisse der Testmessungen des Datenverkehrs zwischen dem Administrationsserver und dem verwalteten Gerät während der Ausführung verschiedener Szenarien.

Die Synchronisierung des Geräts mit dem Administrationsserver erfolgt standardmäßig einmal alle 15 Minuten oder seltener. Wenn Sie jedoch die Einstellungen einer Richtlinie oder einer Aufgabe auf dem Administrationsserver ändern, wird eine vorzeitige Synchronisierung der Geräte vorgenommen, auf die diese Richtlinie (Aufgabe) angewendet wird, und die neuen Einstellungen werden an die Geräte übermittelt.

Datenverkehr zwischen dem Administrationsserver und dem verwalteten Gerät

Szenario	Datenverkehr vom Administrationsserver zu jedem verwalteten Gerät	Datenverkehr von jedem verwalteten Gerät zum Administrationsserver
Installation von Kaspersky Endpoint Security für Linux mit den aktualisierten Datenbanken	390 MB	3,3 MB
Installation des Administrationsagenten	75 MB	397 KB
Gleichzeitige Installation des Administrationsagenten und Kaspersky Endpoint Security für Linux	459 MB	3.6 MB
Erstmaliges Update der Antiviren-Datenbanken ohne Update der Datenbanken im Paket (bei Ablehnung der Teilnahme an Kaspersky Security Network)	113 MB	1,8 MB
Tägliches Update der Antiviren-Datenbanken (bei aktivierter Teilnahme an Kaspersky Security Network)	22 MB	373 MB
Erstmalige Synchronisierung vor dem Datenbanken-Update auf dem Gerät (Übermittlung von Richtlinien und Aufgaben)	382 KB	446 KB
Erstmalige Synchronisierung nach dem Datenbanken-Update auf dem Gerät	20 KB	157 KB
Synchronisierung bei fehlenden Änderungen auf dem Administrationsserver (nach Zeitplan)	18 KB	23 KB
Synchronisierung bei Änderung einer Einstellung in der Gruppenrichtlinie (vorzeitig, sofort nach der Änderung)	19 KB	20 KB
Synchronisierung bei Änderung einer Einstellung in der Gruppenaufgabe (vorzeitig, sofort nach der Änderung)	14 KB	11 KB
Erzwungene Synchronisierung	110 KB	109 KB
Ereignis **Virus gefunden** (1 Virus)	44 KB	50 KB
Ereignis **Virus gefunden** (10 Viren)	58 KB	77 KB

Szenario	Datenverkehr vom Administrationsserver zu jedem verwalteten Gerät	Datenverkehr von jedem verwalteten Gerät zum Administrationsserver
Einmaliger Datenverkehr nach Aktivierung der Programm-Registry-Liste	bis zu 10 KB	bis zu 12 KB
Täglicher Datenverkehr, wenn die Programm-Registry-Liste aktiviert ist	bis zu 840 KB	bis zu 1 MB

Mittleren Verbrauch von Datenverkehr in 24 Stunden

Die durchschnittliche Nutzung des Datenverkehrs stellt sich zwischen dem Administrationsserver und einem verwalteten Gerät innerhalb von 24-Stunden wie folgt dar:

- Der Datenverkehr vom Administrationsserver zum verwalteten Gerät beträgt 840 KB.
- Der Datenverkehr vom verwalteten Gerät zum Administrationsserver beträgt 1 MB.

Der Datenverkehr wurde unter folgenden Bedingungen gemessen:

- Auf dem verwalteten Gerät waren Administrationsagent und Kaspersky Endpoint Security für Linux installiert.
- Dem Gerät wurde kein Verteilungspunkt zugewiesen.
- Das Schwachstellen- und Patch-Management war nicht aktiviert.
- Das Synchronisierungsintervall mit dem Administrationsserver betrug 15 Minuten.

Bekannte Probleme

Kaspersky Security Center Linux besitzt folgende Einschränkungen, die für die Verwendung der Anwendung nicht kritisch sind:

- 8994760: Wenn Sie über Zugriffsrechte für virtuelle Administrationsserver verfügen, aber nicht für den primären Administrationsserver, und sich bei Kaspersky Security Center Linux anmelden möchten, wird ein Fehler mit der falschen Fehlermeldung **Ihre Anfrage kann momentan nicht verarbeitet werden. Bitte warten Sie einen Augenblick und versuchen Sie es später erneut** angezeigt. Die korrekte Fehlermeldung lautet: **Überprüfen Sie Ihre Zugriffsrechte. Sie dürfen nur Zugriffsrechte für den primären Server oder für einen der virtuellen Server besitzen. Kontaktieren Sie den Hauptadministrator und versuchen Sie es anschließend erneut**

- 10085767: Bei der Migration zu Kaspersky Security Center Linux wird der Berichtsumfang möglicherweise falsch angezeigt.

- 10292104: Im Abschnitt **Alarme** werden möglicherweise keine Alarme angezeigt.

- 10308380: Wenn Sie nach dem Erstellen einer Programmkategorie versuchen, deren Eigenschaften direkt vom Bestätigungsdialog mittels der Schaltfläche **OK** zu öffnen, wird das Eigenschaftenfenster nicht geöffnet.

- 10253149: Wenn Sie bei Anwendungsrichtlinien auf der Registerkarte **Konfiguration von Ereignissen** zum Abschnitt **Warnung** wechseln und anschließend auf den Ereignistyp **Aufgabe angehalten** klicken, wird das Dropdown-Menü **Mehr anzeigen** nicht angezeigt.

- 10127434: Wenn Sie in Kaspersky Security Center Web Console auf dem primären Administrationsserver angemeldet sind, den Abschnitt **Aufgaben** öffnen und anschließend das Hierarchiefenster öffnen, wird der virtuelle Server als primärer Server angezeigt.

- 9302142: Die Option **Administrationsagent als Verbindungs-Gateway in der DMZ verwenden** wird für Microsoft Windows on Arm nicht unterstützt.

- 9065814: Beim Versuch einer Domänenauthentifizierung von einem Windows-Gerät in eine Samba 4-Domäne kann ein Fehler auftreten.

- 9335676: Wenn in einem hochverfügbaren DBMS-Cluster der primäre Knoten gewechselt wird, ist anschließend möglicherweise der Zugriff auf die Kaspersky Security Center Web Console nicht mehr verfügbar oder stark verzögert. Wenn die Kaspersky Security Center Web Console länger als 10 Minuten nicht erreichbar ist, starten Sie den IAM-Dienst mit dem folgenden Befehl neu:

  ```
  systemctl restart kliam_srv.service
  ```

- 9157005, 9157085: Wenn die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* auf einem verwalteten Windows-Gerät mit aktivierter Option **Installation beim Neustart bzw. beim Herunterfahren des Geräts beginnen** ausgeführt wird, kann die Aufgabe mit einer Fehlermeldung fehlschlagen. Dieses Problem kann auftreten, wenn eine große Zahl an Updates zur Installation geplant sind. Um dieses Problem zu beheben, führen Sie die Aufgabe ohne aktivierte Option **Installation beim Neustart bzw. beim Herunterfahren des Geräts beginnen** aus.

- 9272534: Wenn die Tabelle der Benutzer mehr als 50.000 Benutzer enthält, werden nur die ersten 50.000 Benutzer angezeigt. Alle weiteren Benutzer werden nicht angezeigt.

- 9291235: Nach der Wiederherstellung eines Backups auf dem Administrationsserver Version 16.1 zeigt die Kaspersky Security Center Web Console die Anmeldeseite. Nach erfolgreicher Authentifizierung wird ein Einmal-Sicherheitscode für die Zwei-Faktor-Authentifizierung angefordert. Wenn ein gültiger Einmal-Sicherheitscode eingegeben wird, wird eine Fehlermeldung angezeigt, die darauf hinweist, dass der Einmal-Sicherheitscode falsch ist. Warten Sie in diesem Fall einige Minuten und aktualisieren Sie dann die Seite manuell, um die Anmeldung bei der Kaspersky Security Center Web Console erneut zu versuchen. Sobald der Wiederherstellungsprozess vollständig abgeschlossen ist, wird die Authentifizierung beim nächsten Versuch erfolgreich sein.

- 7939561: Wenn Sie versuchen, ein geschütztes Benutzerkonto zu ändern, führt das Klicken auf die Schaltfläche **Abbrechen** im Fenster zur Eingabe von Anmeldeinformationen zum **Schutz des Benutzerkontos** zu einem Fehler.

- 8562938: Durch Öffnen des Ports für mobile Geräte in den Eigenschaften der Richtlinie des Administrationsservers wird die Funktion zur Verwaltung mobiler Geräte nicht aktiviert und es wird kein Mobilgerät-Zertifikat generiert. Um die Funktion zur Verwaltung mobiler Geräte zu aktivieren, muss der Port für mobile Geräte in den Eigenschaften des Administrationsservers geöffnet sein.

- 8732282: Für einen Benutzer, der in den Kontoeigenschaften in Active Directory die Option **Benutzer kann das Kennwort nicht ändern** aktiviert hat, wird die Antwortaktion **Kennwort zurücksetzen** in Active Directory nicht ausgeführt. Der Administrator des Domänencontrollers muss entweder die Option **Benutzer kann das Kennwort nicht ändern** deaktivieren oder das Kennwort manuell zurücksetzen. Dieses Problem tritt auf, wenn Sie über die Lizenz Kaspersky Next XDR Optimum verfügen, die Integrität mit Active Directory aktiviert ist und der Benutzer zu einer Active Directory-Sicherheitsgruppe gehört.

- 8688182: Wenn für den Benutzer die Option **Kennwort läuft nie ab** in Active Directory in den Kontoeigenschaften aktiviert ist, wird nach dem Ausführen der Antwortreaktion **Kennwort zurücksetzen** die Option **Kennwort läuft nie ab** deaktiviert und der Benutzer muss das Domänenkennwort bei der nächsten Anmeldung ändern. Dieses Problem tritt auf, wenn Sie über die Lizenz Kaspersky Next XDR Optimum verfügen, die Integrität mit Active Directory aktiviert ist und der Benutzer zu einer Active Directory-Sicherheitsgruppe gehört.

- 8703857: Die Verbindung mit dem Proxyserver für die Kaspersky Security Center Web Console und die Web-Plug-ins zur Verwaltung wird nur dann hergestellt, wenn der Proxyserver die einfache Authentifizierung unterstützt.

- 7911778: Wenn Sie die Aufgabe **Remote-Deinstallation einer Anwendung** ausführen, um den Administrationsagenten auf einem Gerät zu deinstallieren, das unter einem Betriebssystem mit ARM-Architektur läuft und dessen Uhrzeit nicht mit dem Administrationsserver synchronisiert ist, ändert sich der Aufgabenstatus selbst dann nicht von **Wird ausgeführt** zu **Abgeschlossen**, wenn der Administrationsagent erfolgreich vom Gerät deinstalliert wurde. Um dieses Problem zu beheben, müssen Sie vor dem Ausführen der Aufgabe **Remote-Deinstallation einer Anwendung** die Uhrzeit des Geräts mit installiertem Administrationsagenten mit der Uhrzeit des Geräts mit dem Administrationsserver synchronisieren.

- 6896585: Ein verwaltetes Gerät kann keine Verbindung zu KSN über den KSN-Proxy-Dienst herstellen, wenn Kaspersky Security Center Linux auf einem Gerät installiert ist, dessen Name kyrillische Zeichen enthält.

- 7523299: Der Administrationsagent wird auf einem verwalteten Gerät mit CentOS 6.6 nicht neu gestartet, nachdem sein Prozess durch einen Kill-Befehl beendet wurde.

- 7835858: Wenn Sie in Kaspersky Security Center Web Console Version 15.2 eine Aufgabe mit den **Zeitplaneinstellungen Alle N Tage** und Nach Wochentagen erstellen und die Aufgabe anschließend in einer früheren Version der Kaspersky Security Center Web Console oder Verwaltungskonsole öffnen (etwa wenn die Aufgabe auch auf sekundären Administrationsservern angewendet wird, die sowohl Linux-basierte als auch Windows-basierte Administrationsserver sein können), werden die Zeitplaneinstellungen möglicherweise falsch dargestellt, oder es kann ein Fehler auftreten.

- 7208621: Wenn Sie die Aufgabe *Download von Updates in die Datenverwaltungen der Verteilungspunkte* oder *Update-Prüfung* importieren, ist die Option **Wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll** aktiviert. Diese Aufgaben können weder einer Geräteauswahl noch bestimmten Geräten zugewiesen werden. Wenn Sie die Aufgabe *Download von Updates in die Datenverwaltungen der Verteilungspunkte* oder *Update-Prüfung* bestimmten Geräten zuweisen, wird die Aufgabe fehlerhaft importiert.

- 6511063: Wenn eine Anwendung aus dem Abschnitt **Programm-Registry** auf einem Linux-Gerät gefunden wurde, enthalten die Anwendungseigenschaften keine Informationen über zugehörige ausführbare Dateien.

- 5915107: Bei Berichten im Letter-Format kann ein Seitenumbruch eine Textzeile horizontal unterbrechen.

- 5556109: Ein verwaltetes Gerät, dass über mehr als einen Netzwerkadapter verfügt, übermittelt an den Administrationsserver die MAC-Adressinformationen von dem Netzwerkadapter, der nicht zum Herstellen der Verbindung mit dem Administrationsserver verwendet wird.

- 9093038: Wenn der Administrationsserver von Kaspersky Security Center Linux nach der Installation nicht startet und das Protokoll des Betriebssystems einen 213/SECUREBITS-Fehler mit Bezug auf kladminserver_srv.service enthält, führen Sie die folgenden Befehle als Superuser aus:

  ```
  mkdir -p /etc/systemd/system/kladminserver_srv.service.d
  echo "[Service]" > /etc/systemd/system/kladminserver_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kladminserver_srv.service.d/override.conf
  mkdir -p /etc/systemd/system/klwebsrv_srv.service.d
  echo "[Service]" > /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/klwebsrv_srv.service.d/override.conf
  ```

  Wenn die Kaspersky Security Center Web Console nach der Installation nicht startet und das Protokoll des Betriebssystems einen 213/SECUREBITS -Fehler mit Bezug auf KSCWebConsole.service enthält, führen Sie die folgenden Befehle als Superuser aus:

  ```
  mkdir -p /etc/systemd/system/KSCSvcWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCSvcWebConsole.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleManagement.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleManagement.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsoleNATS.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsoleNATS.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsolePlugin.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsolePlugin.service.d/override.conf
  mkdir -p /etc/systemd/system/KSCWebConsole.service.d
  echo "[Service]" > /etc/systemd/system/KSCWebConsole.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/KSCWebConsole.service.d/override.conf
  ```

  Wenn der kliam_srv-Dienst nach der Installtion nicht gestartet wird und das Betriebssystem-Protokoll den 213/SECUREBITS-Fehler enthält, der sich auf diesen Dienst bezieht, führen Sie die folgenden Befehle als Superuser aus:

  ```
  mkdir -p /etc/systemd/system/kliam_srv.service.d
  echo "[Service]" > /etc/systemd/system/kliam_srv.service.d/override.conf
  echo "AmbientCapabilities=CAP_IPC_LOCK" >> /etc/systemd/system/kliam_srv.service.d/override.conf
  ```

- 9165434: Die NTLM-Authentifizierung funktioniert nicht für Benutzerkonten innerhalb der Benutzergruppe "Geschützte Benutzer".

Anfrage an den Technischen Support

Dieser Abschnitt beschreibt, wie und unter welchen Bedingungen Sie technischen Support erhalten.

So erhalten Sie technischen Support

Wenn Sie weder in der Dokumentation von Kaspersky Security Center Linux noch in den anderen Informationsquellen zu Kaspersky Security Center Linux keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky. Die Mitarbeiter des Technischen Supports beantworten alle Fragen zur Installation und Verwendung von Kaspersky Security Center Linux.

> Kaspersky bietet die Unterstützung für Kaspersky Security Center Linux im Rahmen dessen Lebenszyklus' an (siehe Support-Webseite mit dem Lebenszyklus der Anwendung). Bitte beachten Sie die Support-Richtlinien, bevor Sie sich an den Technischen Support wenden.

Eine Kontaktaufnahme mit dem Technischen Support ist auf folgende Weise möglich:

- Durch das Aufrufen der Website des Technischen Supports
- Durch das Senden einer Anfrage an den Technischen Support über das Portal Kaspersky CompanyAccount

Technischer Support mit Kaspersky CompanyAccount

Kaspersky CompanyAccount ist ein Portal für Unternehmen, die Kaspersky-Programme verwenden. Das Portal Kaspersky CompanyAccount dient der Interaktion zwischen Benutzern und Kaspersky-Experten mithilfe von Online-Anfragen. Mithilfe von Kaspersky CompanyAccount können Sie den Status Ihrer Online-Anfragen verfolgen und eine Chronik mit allen Anfragen speichern.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Mithilfe eines einheitlichen Kontos können Sie die Online-Anfragen der bei Kaspersky registrierten Mitarbeiter zentral verwalten und die Berechtigungen dieser Mitarbeiter für Kaspersky CompanyAccount verwalten.

Das Portal Kaspersky CompanyAccount ist in den folgenden Sprachen verfügbar:

- Englisch
- Spanisch
- Italienisch
- Deutsch
- Polnisch
- Portugiesisch

- Russisch
- Französisch
- Japanisch

Weitere Informationen über Kaspersky CompanyAccount finden Sie auf der Webseite des Technischen Supports.

Dump-Dateien des Administrationsservers abrufen

Die Dump-Dateien des Administrationsservers enthalten alle Informationen über die Prozesse des Administrationsservers zu einem bestimmten Zeitpunkt. Die Dump-Dateien des Administrationsservers werden im Verzeichnis /var/lib/systemd/coredump gespeichert. Die Dump-Dateien bleiben so lange gespeichert, wie Kaspersky Security Center Linux verwendet wird. Wenn Kaspersky Security Center Linux entfernt wird, werden auch die Dump-Dateien endgültig gelöscht. Dump-Dateien werden nicht automatisch an Kaspersky übertragen.

Wenn der Administrationsserver abstürzt, können Sie sich an den Technischen Support von Kaspersky wenden. Ein Spezialist des Technischen Supports bittet Sie dann womöglich, die Dump-Dateien des Administrationsservers zur weiteren Analyse an Kaspersky zu senden.

Dump-Dateien können personenbezogene Daten enthalten. Es wird empfohlen, die Informationen vor dem Senden an Kaspersky vor unbefugtem Zugriff zu schützen.

Weitere Informationsquellen zu dieser Anwendung

Seite von Kaspersky Security Center Linux auf der Website von Kaspersky

Auf der Seite von Kaspersky Security Center Linux des Kaspersky-Webauftritts finden Sie allgemeine Informationen über die Anwendung, ihre Funktionen und Besonderheiten.

Seite von Kaspersky Security Center Linux in der Wissensdatenbank

Die *Wissensdatenbank* ist ein Abschnitt der Website des Technischen Supports von Kaspersky.

Auf der Seite von Kaspersky Security Center Linux in der Wissensdatenbank finden Sie Artikel mit nützlichen Informationen, Tipps und Antworten auf häufige Fragen zum Kauf, zur Installation und zur Nutzung der Anwendung.

Neben Fragen zu Kaspersky Security Center Linux können die Artikel auch andere Anwendungen von Kaspersky betreffen. Artikel in der Wissensdatenbank können auch Neuigkeiten über den Technischen Support enthalten.

In der Community über Kaspersky-Anwendungen diskutieren

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie diese mit den Experten von Kaspersky und mit anderen Benutzern in unserem Forum diskutieren.

Im Forum können Sie Diskussionsthemen nachlesen, Kommentare schreiben und neue Diskussionsthemen erstellen.

> Um auf die Website-Ressourcen zuzugreifen, ist eine Internetverbindung erforderlich.

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support.

Glossar

Administrationsagent

Eine Komponente von Kaspersky Security Center Linux, mit deren Hilfe die Interaktion zwischen dem Administrationsserver und den Kaspersky-Anwendung ermöglicht wird, die auf einem bestimmten Netzwerk-Knoten (Workstation oder Server) installiert sind. Diese Komponente ist für alle von dem Unternehmen entwickelten Anwendung für Microsoft® Windows® einheitlich. Für Kaspersky-Anwendungen, die für Unix-artige Betriebssysteme und macOS entwickelt wurden, gibt es separate Versionen des Administrationsagenten.

Administrationsgruppe

Ein Satz von Geräten, die nach Funktion und installierten Kaspersky-Anwendungen gruppiert sind. Geräte sind zur erleichterten Verwaltung als einzelne Entität gruppiert. Eine Gruppe kann andere Gruppen beinhalten. Für jede installierte Anwendung in der Gruppe können Gruppenrichtlinien und Gruppenaufgaben erstellt werden.

Administrationsserver

Eine Komponente von Kaspersky Security Center Linux, die Informationen über alle Kaspersky-Anwendungen, die innerhalb des Unternehmensnetzwerks installiert sind, zentral speichert. Sie kann auch zur Verwaltung dieser Anwendungen verwendet werden.

Administrationsserver-Client (Client-Gerät)

Gerät, Server oder Workstation, auf welchem bzw. welcher der Administrationsagent installiert ist und verwaltete Kaspersky-Anwendungen ausgeführt werden.

Administrator des Anbieters

Mitarbeiter eines Anbieters von Antiviren-Schutz. Dieser Administrator führt Installations- und Verwaltungsaufträge für Antiviren-Schutzsysteme auf der Grundlage von Antiviren-Produkten von Kaspersky durch und bietet darüber hinaus technischen Support für Kunden.

Administrator von Kaspersky Security Center Linux

Die Person, die über das zentralisierte Remote-Verwaltungssystem Kaspersky Security Center Linux die Anwendungsvorgänge verwaltet.

Administrator-Arbeitsplatz

Ein Gerät, auf dem Sie Kaspersky Security Center Web Console öffnen. Diese Komponente stellt eine Verwaltungsschnittstelle von Kaspersky Security Center Linux bereit.

Der Administrator-Arbeitsplatz wird zur Konfiguration und Verwaltung der Serverseite von Kaspersky Security Center Linux verwendet. Mithilfe des Administrator-Arbeitsplatzes erstellt und verwaltet der Administrator ein zentralisierten Antiviren-Schutzsystem für ein Unternehmens-LAN auf der Grundlage von Kaspersky-Anwendungen.

Administratorberechtigungen

Stufe der Benutzerberechtigungen und Rechte, die für die Verwaltung von Exchange-Objekten innerhalb einer Exchange-Organisation erforderlich sind.

Aktiver Schlüssel

Ein Schlüssel, der momentan von der Anwendung verwendet wird.

Anbieter von Antiviren-Schutz

Ein Unternehmen, das für ein Kundenunternehmen einen Antiviren-Schutz auf der Grundlage von Lösungen von Kaspersky bereitstellt.

Antiviren-Datenbanken

Datenbanken, die Informationen über diejenigen Bedrohungen der Computersicherheit enthalten, die Kaspersky zum Zeitpunkt des Erscheinens der Antiviren-Datenbanken bekannt sind. Durch die Eintragungen in den Antiviren-Datenbanken kann in den untersuchten Objekten schädlicher Code erkannt werden. Antiviren-Datenbanken werden von den Experten von Kaspersky erstellt und stündlich aktualisiert.

App Store

Komponente von Kaspersky Security Center Linux. Der App Store wird zur Installation von Apps auf Android-Geräten von Benutzern verwendet. Der App Store erlaubt Ihnen, die APK-Dateien von Apps und Links zu Apps in Google Play zu veröffentlichen.

Aufgabe

Funktionen, die eine Kaspersky-Anwendung ausführt, werden als Aufgaben implementiert, beispielsweise: Echtzeitschutz von Dateien, Vollständige Untersuchung des Computers und Datenbanken-Update.

Aufgabe für eine Reihe von Geräten

Aufgabe, die einer Auswahl von Client-Geräten aus beliebigen Administrationsgruppen zugewiesen ist und auf diesen Geräten ausgeführt wird.

Aufgabeneinstellungen

Anwendungseinstellungen, die spezifisch für die einzelnen Aufgabentypen sind.

Authentifizierungsagent

Schnittstellen, mit der Sie die Authentifizierung für den Zugriff auf verschlüsselte Festplatten abschließen und das Betriebssystem nach der Verschlüsselung der startbaren Festplatte laden können.

Backup-Ordner

Spezieller Ordner zum Speichern von Kopien der Daten des Administrationsservers, die mithilfe des Backup-Tools erstellt werden.

Broadcast-Domäne

Logischer Bereich eines Netzwerks, in dem alle Knoten mithilfe eines Broadcast-Kanals auf OSI-Ebene (Open Systems Interconnection Basic Reference Model) Daten austauschen können.

Client-Administrator

Mitarbeiter eines Kundenunternehmens, der für die Überwachung des Antiviren-Schutzstatus verantwortlich ist.

Cloud Discovery

Cloud Discovery ist eine Komponente des Cloud Access Security Brokers (CASB), der die Cloud-Infrastruktur eines Unternehmens schützt. Cloud Discovery verwaltet den Benutzerzugriff auf Cloud-Dienste. Solche Cloud-Dienste sind beispielsweise Microsoft Teams, Salesforce und Microsoft Office 365. Die Cloud-Dienste werden in Kategorien wie *Datenaustausch*, *Messenger* oder *E-Mail* eingeteilt.

Daten-Backup des Administrationsservers

Kopieren der Daten des Administrationsservers als Backup und zur anschließenden Wiederherstellung mithilfe des Backup-Tools. Das Tool kann Folgendes speichern:

- Administrationsserver-Datenbank (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse)
- Konfigurationsdaten über die Struktur von Administrationsgruppen und Client-Geräten
- Datenverwaltung der Installationsdateien zur Remote-Installation von Anwendungen (Inhalt der Ordner Pakete, Update-Deinstallation)
- Zertifikat des Administrationsservers

Demilitarisierte Zone (DMZ)

Die demilitarisierte Zone ist ein Segment eines lokalen Netzwerks, das Server enthält, die auf Anfragen aus dem globalen Internet antworten. Um die Sicherheit des lokalen Netzwerks einer Organisation zu gewährleisten, wird der Zugriff auf das LAN aus der demilitarisierten Zone mithilfe einer Firewall geschützt.

Direkte Anwendungsverwaltung

Anwendungsverwaltung über eine lokale Schnittstelle.

Ereignis-Datenverwaltung

Ein Teil der Administrationsserver-Datenbank. Dort werden Informationen über in Kaspersky Security Center Linux auftretende Ereignisse gespeichert.

Ereigniskategorie des Patches

Attribut des Patches. Es gibt fünf Ereigniskategorien für Microsoft-Patches und Drittanbieter-Patches:

- Kritisch
- Hoch
- Normal
- Niedrig
- Unbekannt

Die Ereigniskategorie eines Drittanbieter-Patches oder Microsoft-Patches wird durch die ungünstigste Signifikanz unter den Schwachstellen bestimmt, die der Patch beheben soll.

Gerätebesitzer

Der Gerätebesitzer ist ein Benutzer, an den sich der Administrator wenden kann, wenn Bedarf zur Durchführung bestimmter Operationen auf einem Gerät besteht.

Geteiltes Zertifikat

Ein Zertifikat, das zur Identifizierung des mobilen Geräts des Benutzers dient.

Gruppenaufgabe

Aufgabe, die für eine Administrationsgruppe definiert und auf allen Client-Geräten innerhalb dieser Administrationsgruppe ausgeführt wird.

Gültigkeitsdauer der Lizenz

Zeitraum, in dem Ihnen die Funktionen der Anwendung zur Verfügung stehen und Sie berechtigt sind, zusätzliche Leistungen in Anspruch zu nehmen. Die Ihnen zur Verfügung stehenden Leistungen hängen vom Lizenztyp ab.

Home-Administrationsserver

Der Home-Administrationsserver ist der Administrationsserver, der während der Installation des Administrationsagenten festgelegt wurde. Der Home-Administrationsserver kann in Einstellungen der Verbindungsprofile des Administrationsagenten verwendet werden.

HTTPS

Sicheres Protokoll zur Datenübertragung mittels Verschlüsselung zwischen einem Browser und einem Webserver. Um Zugriff auf beschränkte Informationen, wie etwa Unternehmensdaten oder Finanzdaten, zu erhalten, wird HTTPS verwendet.

Identitäts- und Zugriffsverwaltung (IAM)

Eine Komponente des Administrationsservers, die Ihnen die Verwendung der Domänenauthentifizierung (Single Sign-On) ermöglicht. Ein Benutzer, der die Funktion zum Single Sign-on verwendet, kann die sichere Authentifizierung in Kaspersky Security Center Web Console aktivieren, ohne das Kennwort im Unternehmensnetzwerk erneut eingeben zu müssen.

Inkompatible Anwendung

Eine Antiviren-Anwendung eines Drittanbieters oder eine Kaspersky-Anwendung, welche die Verwaltung über Kaspersky Security Center Linux nicht unterstützt.

Installationspaket

Zusammenstellung von Dateien, die für die Remote-Installation einer Kaspersky-Anwendung mithilfe des Remote-Verwaltungssystems von Kaspersky Security Center erstellt wurde. Das Installationspaket enthält eine Reihe von Einstellungen, die für die Installation und Inbetriebnahme der Anwendung nach der Installation benötigt werden. Die Einstellungen entsprechen der Standardkonfiguration der Anwendung. Das Installationspaket wird mithilfe von Dateien mit der Erweiterung .kpd und .kud erstellt, die im Lieferumfang der Anwendung enthalten sind.

Interne Benutzer

Die Benutzerkonten der internen Benutzer werden für die Arbeit mit den virtuellen Administrationsservern verwendet. Innerhalb der Funktionen von Kaspersky Security Center Linux verfügen die internen Benutzer über die Berechtigungen tatsächlicher Benutzer.

Benutzerkonten der internen Benutzer werden nur innerhalb von Kaspersky Security Center Linux erstellt und verwendet. Informationen über die internen Benutzer werden nicht auf das Betriebssystem übertragen. Die Authentifizierung der internen Benutzer erfolgt über Kaspersky Security Center Linux.

iOS MDM-Gerät

Mobiles Gerät, das über das iOS MDM-Protokoll mit dem iOS MDM-Server verbunden ist. Geräte mit dem Betriebssystem iOS können mithilfe des iOS MDM-Protokolls verbunden und verwaltet werden.

iOS MDM-Server

Komponente von Kaspersky Security Center, die auf einem Client-Gerät installiert ist, die eine Verbindung von mobilen iOS-Geräten mit dem Administrationsserver und die Verwaltung von mobilen iOS-Geräten über Apple Push Notifications (APNs) ermöglicht.

JavaScript

Programmiersprache, mit der die Leistungsfähigkeit von Webseiten erweitert wird. Webseiten, die mithilfe von JavaScript erstellt wurden, können Funktionen (beispielsweise die Ansicht von Schnittstellenelementen ändern oder zusätzliche Fenster öffnen) ausführen, ohne die Webseite mit neuen Daten aus einem Webserver zu aktualisieren. Um Seiten anzuzeigen, die mithilfe von JavaScript erstellt wurden, aktivieren Sie die Unterstützung von JavaScript in der Konfiguration Ihres Browsers.

Kaspersky Private Security Network (KPSN)

Die Lösung Kaspersky Private Security Network gewährt Benutzern von Geräten, auf denen Kaspersky-Anwendungen installiert sind, Zugriff auf die Reputationsdatenbanken von Kaspersky Security Network sowie auf andere statistische Daten, ohne dass Daten von ihren Geräten an Kaspersky Security Network gesendet werden müssen. Kaspersky Private Security Network richtet sich an Unternehmenskunden, die aus einem der folgenden Gründe nicht an Kaspersky Security Network teilnehmen können:

- Die Geräte haben keine Internetverbindung.
- Die Übermittlung von Daten an einen Punkt außerhalb des Landes oder des lokalen Unternehmensnetzwerks ist gesetzlich oder aufgrund von Sicherheitsrichtlinien des Unternehmens untersagt.

Kaspersky Security Center Linux Webserver

Komponente von Kaspersky Security Center Linux, die gemeinsam mit dem Administrationsserver installiert wird. Der Webserver dient dazu, autonome Installationspakete, iOS MDM-Profile sowie Dateien aus einem freigegebenen Ordner im Netzwerk zu übertragen.

Kaspersky Security Center Operator

Benutzer, der den Status und Betrieb eines Schutzsystems überwacht, das mithilfe von Kaspersky Security Center verwaltet wird.

Kaspersky Security Center System Health Validator (SHV)

Komponente von Kaspersky Security Center Linux, die zur Überprüfung der Einsatzfähigkeit des Betriebssystems im Fall von gleichzeitigem Betrieb von Kaspersky Security Center Linux und Microsoft NAP dient.

Kaspersky-Update-Server

HTTP(S)-Server bei Kaspersky, von denen Programme von Kaspersky Updates für Datenbanken und Programm-Module herunterladen.

Konfigurationsprofil

Richtlinie, die eine Zusammenstellung von Einstellungen und Einschränkungen für ein mobiles iOS MDM-Gerät enthält.

Lightweight Nagent (LWNGT)

Ein Protokoll für die Interaktion mit Kaspersky Endpoint Security auf Mobilgeräten. LWNGT (auch mobiles Protokoll genannt) fungiert als Administrationsagent, ohne dass der Administrationsagent tatsächlich auf Mobilgeräten installiert sein muss.

Lokale Aufgabe

Aufgabe, die auf einem einzelnen Client-Computer definiert wurde und ausgeführt wird.

Lokale Installation

Installation einer Sicherheitsanwendung auf einem Gerät in einem Unternehmensnetzwerk, die entweder den manuellen Start der Installation über das Programmpaket der Sicherheitsanwendung oder den manuellen Start eines veröffentlichten Installationspakets, das zuvor auf das Gerät heruntergeladen wurde, voraussetzt.

Manuelle Installation

Installation einer Sicherheitsanwendung aus dem Programmpaket auf einem Gerät im Unternehmensnetzwerk. Manuelle Installation erfordert die Einbeziehung eines Administrators oder anderen IT-Spezialisten. Im Normalfall wird eine manuelle Installation durchgeführt, wenn die Remote-Installation mit einem Fehler beendet wurde.

Network Location Awareness (NLA)

Ein Windows-Dienst, der einem Betriebssystem hilft, das aktuelle Netzwerk zu identifizieren. NLA erkennt Änderungen des Netzwerks und passt die Sicherheitskonfiguration des Geräts an.

Netzwerk-Antiviren-Schutz

Satz von technischen und organisatorischen Maßnahmen, die das Risiko senken, dass Viren und Spam in das Netzwerk einer Organisation eindringen, und die Netzwerkangriffe, Phishing und andere Bedrohungen verhindern. Die Sicherheit des Netzwerks steigt, wenn Sie Sicherheitsanwendungen und Dienste nutzen, und wenn Sie die Sicherheitsrichtlinie des Unternehmens übernehmen und einhalten.

Netzwerk-Schutzstatus

Aktueller Schutzstatus, der die Sicherheit der Geräte im Unternehmensnetzwerk definiert. Der Status des Netzwerk-Schutzstatus beinhaltet Faktoren wie installierte Sicherheitsanwendungen, Verwendung von Lizenzschlüsseln sowie Anzahl und Typen der gefundenen Bedrohungen.

Profil

Zusammenstellung von Einstellungen für mobile Geräte mit Exchange, die deren Verhalten definieren, wenn sie mit einem Microsoft Exchange-Server verbunden sind.

Programmeinstellungen

Anwendungseinstellungen, die für alle Aufgabentypen gleich sind und den Gesamtbetrieb der Anwendung regeln, zum Beispiel Leistungseinstellungen, Berichtseinstellungen und Backup-Einstellungen.

Provisioning-Profil

Zusammenstellung von Einstellungen für die Ausführung von Anwendungen auf mobilen iOS-Geräten. Ein Provisioning-Profil enthält Informationen zur Lizenz und ist mit einer bestimmten Anwendung verbunden.

Remote-Installation

Installation von Kaspersky-Anwendungen über die von Kaspersky Security Center Linux bereitgestellten Dienste.

Richtlinie

Eine Richtlinie bestimmt die Einstellungen einer Anwendung und verwaltet die Möglichkeit, diese Anwendung auf Computern innerhalb einer Administrationsgruppe zu konfigurieren. Für jede Anwendung muss eine eigene Richtlinie erstellt werden. Sie können mehrere Richtlinien für Anwendungen, die auf Computern in mehreren Administrationsgruppen installiert sind, erstellen, es kann jedoch innerhalb einer Administrationsgruppe immer nur eine Richtlinie auf eine Anwendung angewendet werden.

Rollengruppe

Gruppe von Benutzern von mobilen Geräten mit Exchange ActiveSync, denen identische Administratorberechtigungen gewährt wurden.

Schlüsseldatei

Datei im Format xxxxxxxx.key, die ermöglicht, eine Kaspersky-Anwendung unter eine Test- oder kommerziellen Lizenz zu nutzen.

Schutzstatus

Aktueller Schutzstatus, der die Stufe der Computersicherheit widerspiegelt.

Schwachstelle

Ein Fehler in einem Betriebssystem oder einem Programm, der von Entwicklern von Schadsoftware benutzt werden kann, um in das Betriebssystem oder Programm einzudringen und dessen Integrität zu gefährden. Das Vorliegen einer großen Anzahl von Schwachstellen in einem Betriebssystem macht dieses unzuverlässig, da Viren, die in das Betriebssystem eingedrungen sind, zu Ausführungsfehlern im System selbst sowie in den installierten Programmen führen können.

Signifikanz des Ereignisses

Eigenschaft eines Ereignisses, das während des Betriebs einer Kaspersky-Anwendung aufgetreten ist. Es gibt folgende Varianten für die Signifikanz:

- Kritisches Ereignis
- Funktionsfehler
- Warnung
- Information

Ereignisse desselben Typs können abhängig von der Situation, in der das Ereignis aufgetreten ist, unterschiedliche Signifikanzen aufweisen.

SSL

Datenverschlüsselungsprotokoll, das im Internet und in lokalen Netzwerken verwendet wird. Das SSL-Protokoll (Secure Sockets Layer) wird in Web-Anwendungen verwendet, um eine sichere Verbindung zwischen einem Client und einem Server herzustellen.

Update

Das Verfahren zum Ersetzen oder Hinzufügen von neuen Dateien (Datenbanken oder Anwendungsmodule), die von den Kaspersky-Update-Servern abgerufen werden.

Verbindungs-Gateway

Ein *Verbindungs-Gateway* ist ein Administrationsagent, der in einem speziellen Modus ausgeführt wird. Ein Verbindungs-Gateway akzeptiert Verbindungen von anderen Administrationsagenten und tunnelt diese zum Administrationsserver mittels einer eigenen Verbindung zum Server. Anstatt wie gewöhnliche Administrationsagenten selbst eine Verbindung zum Administrationsserver herzustellen, wartet ein Verbindungs-Gateway auf eine Verbindung vom Administrationsserver.

Verfügbares Update

Satz von Updates für Anwendungsmodule von Kaspersky einschließlich kritischer Updates, die sich über einen bestimmten Zeitraum angesammelt haben, und Änderungen an der Anwendungsarchitektur.

Verteilungspunkt

Computer, auf dem der Administrationsagent installiert ist und der zur Update-Verteilung, zur Remote-Installation von Anwendungen und zum Empfangen von Informationen über Computer in einer Administrationsgruppe und/oder Broadcasting-Domäne verwendet wird. Verteilungspunkte dienen dazu, die Belastung auf dem Administrationsserver während der Update-Verteilung zu verringern und den Netzwerkdatenverkehr zu optimieren. Verteilungspunkte können automatisch vom Administrationsserver oder manuell vom Administrator zugewiesen werden. Der Verteilungspunkt war in früheren Versionen als Update-Agent bekannt.

Verwaltete Geräte

Geräte in Unternehmensnetzwerken, die in einer Administrationsgruppe enthalten sind.

Verwaltungskonsole

Eine Komponente des Windows-basierten Kaspersky Security Center (auch "MMC-basierte Verwaltungskonsole" genannt). Diese Komponente stellt eine Benutzeroberfläche für die administrativen Dienste des Administrationsservers und des Administrationsagenten bereit. Die Verwaltungskonsole entspricht der Kaspersky Security Center Web Console.

Virenangriff

Eine Serie von vorsätzlichen Versuchen, ein Gerät mit einem Virus zu infizieren.

Virtueller Administrationsserver

Komponente von Kaspersky Security Center Linux, die zur Verwaltung des Schutzsystems für das Netzwerk eines Kundenunternehmens dient.

Ein virtueller Administrationsserver stellt einen besonderen Fall eines sekundären Administrationsservers dar und weist im Vergleich zu einem physikalischen Administrationsserver folgende Einschränkungen auf:

- Ein virtueller Administrationsserver kann nur auf einem primären Administrationsserver erstellt werden.
- Ein virtueller Administrationsserver verwendet während seines Betriebs die Datenbank des primären Administrationsservers. Aufgaben zum Anlegen eines Daten-Backups und zur Wiederherstellung von Dateien, sowie Aufgaben zur Suche nach Updates und Downloadaufgaben werden von einem virtuellen Administrationsserver nicht unterstützt.
- Für virtuelle Server können keine sekundären Administrationsserver angelegt werden (einschließlich virtueller Server).

Wiederherstellung

Wiederherstellung des ursprünglichen Objekts aus der Quarantäne oder dem Backup in seinem ursprünglichen Ordner, wo das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einem benutzerdefinierten Ordner.

Wiederherstellung der Daten des Administrationsservers

Wiederherstellung der Daten des Administrationsservers aus den Informationen, die mithilfe des Backup-Tools im Backup gespeichert wurden. Das Tool kann Folgendes wiederherstellen:

- Datenbank des Administrationsservers (Richtlinien, Aufgaben, Anwendungseinstellungen, auf dem Administrationsserver gespeicherte Ereignisse)
- Konfigurationsdaten über die Struktur von Administrationsgruppen und Client-Geräten
- Datenverwaltung der Installationsdateien zur Remote-Installation von Anwendungen (Inhalt der Ordner Pakete, Update-Deinstallation)
- Zertifikat des Administrationsservers

Zentralisierte Anwendungsverwaltung

Remote-Anwendungsverwaltung mithilfe der Verwaltungsdienste, die in Kaspersky Security Center bereitgestellt werden.

Zertifikat des Administrationsservers

Das Zertifikat, das der Administrationsserver für folgende Zwecke verwendet:

- Authentifizierung des Administrationsservers beim Verbinden mit Kaspersky Security Center Web Console
- Sichere Interaktion zwischen dem Administrationsserver und den Administrationsagenten auf verwalteten Geräten
- Authentifizierung von Administrationsservern beim Verbinden eines primären Administrationsservers mit einem sekundären Administrationsserver

Das Zertifikat wird bei der Installation des Administrationsservers automatisch erstellt und auf dem Administrationsserver gespeichert.

Zusätzlicher Lizenzschlüssel (oder Reserve-Lizenzschlüssel)

Ein Schlüssel, der das Recht auf Nutzung der Anwendung bestätigt, jedoch im Augenblick nicht aktiviert ist.

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittanbietern finden Sie in der Datei legal_notices.txt, die sich im Installationsverzeichnis der Anwendung befindet.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Adobe, Acrobat, Flash, PostScript und Shockwave sind in den USA und/oder anderen Ländern entweder eingetragene Markenzeichen oder Markenzeichen von Adobe.

AMD, AMD64 sind Markenzeichen oder eingetragene Markenzeichen von Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2 und AWS Marketplace sind Markenzeichen von Amazon.com, Inc. oder von verbundenen Unternehmen.

Apache ist entweder ein eingetragenes Markenzeichen oder ein Markenzeichen der Apache Software Foundation in den USA und anderen Ländern.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime und Touch ID sind Markenzeichen von Apple Inc.

Arm ist ein eingetragenes Markenzeichen von Arm Limited (oder seinen Tochtergesellschaften) in den USA und/oder anderswo.

Die Bluetooth-Wortmarke und die Bluetooth-Logos sind Eigentum der Bluetooth SIG, Inc.

Ubuntu und LTS sind eingetragene Markenzeichen von Canonical Ltd.

Cisco, Cisco Jabber, Cisco Systems und IOS sind eingetragene Markenzeichen von Cisco Systems, Inc. und/oder ihren Tochtergesellschaften in den USA und in anderen Ländern.

Citrix und XenServer sind entweder eingetragene Markenzeichen oder Markenzeichen der Cloud Software Group, Inc. und/oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern.

Corel ist eine Marke oder eingetragene Marke der Corel Corporation und/oder ihrer Tochtergesellschaften in Kanada, den USA und/oder anderen Ländern.

Cloudflare, das Cloudflare-Logo und Cloudflare Workers sind Markenzeichen und/oder eingetragene Markenzeichen von Cloudflare, Inc. in den Vereinigten Staaten und anderen Gerichtsbarkeiten.

Dropbox ist ein Markenzeichen von Dropbox, Inc.

Radmin ist ein eingetragenes Markenzeichen von Famatech.

Firebird ist ein eingetragenes Markenzeichen der Firebird-Stiftung.

Foxit ist ein eingetragenes Markenzeichen der Foxit Corporation.

Das Logo FreeBSD ist ein eingetragenes Warenzeichen der Stiftung The FreeBSD.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Google Public DNS, Hangouts und YouTube sind Markenzeichen von Google LLC.

EulerOS, FusionCompute und FusionSphere sind Markenzeichen von Huawei Technologies Co., Ltd.

Intel, Core und Xeon sind Markenzeichen der Intel Corporation oder ihrer Tochtergesellschaften.

IBM und QRadar sind Markenzeichen der International Business Machines Corporation und in vielen Ländern der Welt eingetragen.

Node.js ist ein Markenzeichen von Joyent, Inc.

Linux ist das eingetragene Markenzeichen von Linus Torvalds in den USA und anderen Ländern.

Logitech ist entweder ein Markenzeichen oder ein eingetragenes Markenzeichen von Logitech in den USA und anderen Ländern.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, PowerShell, PowerPoint, SharePoint, SQL Server, Office 365, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Server, Windows Phone, Windows Vista und Windows Azure sind Markenzeichen der Microsoft-Unternehmensgruppe.

Mozilla, Firefox und Thunderbird sind Markenzeichen der Mozilla Foundation in den USA und anderen Ländern.

Novell ist ein in den USA und anderen Ländern eingetragenes Markenzeichen von Novell Enterprises Inc.

OpenSSL ist ein Markenzeichen der OpenSSL Software Foundation.

OpenVPN ist ein eingetragenes Markenzeichen von OpenVPN, Inc.

Oracle, Java, JavaScript und TouchDown sind eingetragene Markenzeichen von Oracle und/oder von verbundenen Unternehmen.

Parallels, das Parallels-Logo und Coherence sind Markenzeichen oder eingetragene Markenzeichen der Parallels International GmbH.

Chef ist ein Markenzeichen oder eingetragenes Markenzeichen der Progress Software Corporation und/oder einer ihrer Tochtergesellschaften oder verbundenen Unternehmen in den USA und/oder anderen Ländern.

Puppet ist ein Markenzeichen oder eingetragenes Markenzeichen von Puppet, Inc.

Python ist ein Markenzeichen oder eingetragenes Markenzeichen der Python Software Foundation.

Red Hat, Fedora und Red Hat Enterprise Linux sind in den USA und in anderen Ländern Markenzeichen oder eingetragene Markenzeichen von Red Hat Inc oder seinen Tochtergesellschaften.

Ansible ist ein in den USA und anderen Ländern eingetragenes Markenzeichen von Red Hat, Inc.

CentOS ist in den USA und in anderen Ländern ein Markenzeichen oder eingetragene Markenzeichen von Red Hat, Inc oder seinen Tochtergesellschaften.

BlackBerry steht im Besitz von Research In Motion Limited ist in den USA eingetragen. Die Marke kann auch in anderen Ländern angemeldet oder eingetragen sein.

Rocky Linux ist ein Markenzeichen der The Rocky Enterprise Software Foundation.

SAMSUNG ist ein eingetragenes Warenzeichen von SAMSUNG in den USA und anderen Ländern.

Debian ist ein eingetragenes Warenzeichen von Software in the Public Interest, Inc.

Splunk und SPL sind Markenzeichen und eingetragene Markenzeichen von Splunk Inc. in den USA und anderen Ländern.

SUSE ist ein in den USA und anderen Ländern eingetragenes Markenzeichen von SUSE LLC.

Das Markenzeichen Symbian ist Eigentum der Symbian Foundation Ltd.

OpenAPI ist ein Markenzeichen von The Linux Foundation.

UNIX ist ein in den Vereinigten Staaten und in anderen Ländern eingetragenes Markenzeichen. Die Nutzung wird durch die Firma X/Open Company Limited lizenziert.

Zabbix ist ein eingetragenes Markenzeichen von Zabbix SIA.