kaspersky

Kaspersky Security Center 15.1 Linux

Inhalt

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 Programme

Bereitstellung und Konfiguration

- Geräte im Netzwerk finden
- Verteilungspunkte und/oder Verbindungs-Gateways anpassen
- Ersetzen von Sicherheitsanwendungen von Drittanbietern
- Kaspersky-Programme. Zentralisierte Bereitstellung
- Netzwerkschutz konfigurieren

- Kaspersky-Programme. Datenbanken-Update und Update der Programm-Module

Überwachung

- Überwachung und Berichterstattung
- Cloud Discovery

Schwachstellen- und Patch-Management

- Finden und Schließen von Schwachstellen in Programmen von Drittanbietern

Zusätzliche Funktionen

- Ereignisse in SIEM-Systeme exportieren
- Handbuch zur Skalierung (nur Online-Hilfe)

Neuerungen

Kaspersky Security Center 15.1 Linux

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

- Schwachstellen- und Patch-Management für verwaltete Windows-Geräte. Sie können jetzt auf verwalteten Windows-Geräten Updates für installierte Software von Drittanbietern verwalten und Schwachstellen beheben, die in dieser Software 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 und Berichterstattung** des Hauptmenüs hinzugefügt. Im Unterabschnitt **Alarme** können Sie Informationen über erkannte Bedrohungen auf den Endpunktgeräten anzeigen. Die Bedrohungen werden von den Kaspersky-Sicherheitsanwendungen erkannt.
- Kaspersky Security Center Linux kann jetzt als Komponente der Lösung Kaspersky Managed Detection and Response eingesetzt werden.
- Beim Upgrade von Kaspersky Endpoint Security für Windows auf Kaspersky Security for Windows Server ist kein Neustart des Zielgeräts mehr erforderlich.
- 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 eines Programms* 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 im Abschnitt **Angepinnt** ausgewählte Abschnitte der Kaspersky Security Center Web Console für einen schnelleren Zugriff angeheftet 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 weitere 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 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-Programme:
  - 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 Programmkategorie von Kaspersky 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 **Verwaltete 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 verwaltetes Programm.

  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-Programmen als auch Verwaltungs-Web-Plug-Ins direkt in der Benutzeroberfläche von Kaspersky Security Center Linux herunterladen und aktualisieren.
- Standardmäßig werden Informationen über Programme, 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 das Programm 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 Programm-Module 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-Sicherheits-Apps 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 Unternehmensnetzwerk, 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 Cyber Security for Linux Nodes 1.3 als verwaltetes Programm.

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-Sicherheits-Apps auf Geräten in einem Unternehmensnetzwerk installieren, Untersuchungs- und Update-Aufgaben per Fernzugriff ausführen und die Sicherheitsrichtlinien verwalteter Apps 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-Programmen basiert.

- Apps von Kaspersky und anderen Softwareanbietern per Fernzugriff installieren.

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

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

- Benachrichtigungen über kritische Ereignisse bei der Ausführung von Kaspersky-Programmen 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 das Programm von unserer Website herunterladen. Sie erhalten die zur Programmaktivierung erforderlichen Informationen per E-Mail, nachdem der Eingang Ihres Rechnungsbetrags verarbeitet wurde.

Lieferumfang

Sie können das Programm über den Online-Shop von Kaspersky (beispielsweise auf https://www.kaspersky.de) oder über unsere Partnerunternehmen erwerben.

Beim Kauf von Kaspersky Security Center Linux in einem Online-Shop kopieren Sie das Programm von der Website des Online-Shops. Sie erhalten die zur Programmaktivierung erforderlichen Informationen nach Eingang des Rechnungsbetrags per E-Mail.

Hard- und Softwarevoraussetzungen

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

Anforderungen an den Administrationsserver

Mindestvoraussetzungen an die Hardware:

- CPU mit einer Taktfrequenz von 1,4 GHz oder höher.
- RAM: 4 GB.
- Freier Speicherplatz auf dem Datenträger: 10 GB (/var/opt/kaspersky/klnagent_srv).

Die folgenden Betriebssysteme werden unterstützt:

- Debian GNU/Linux 11.x (Bullseye) 64-Bit
- Debian GNU/Linux 12 (Bookworm) 64-Bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 64-Bit
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-Bit
- CentOS Stream 9 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

- 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.10015-37 (operatives Update 7.7) 64-Bit
- Astra Linux Common Edition (operatives Update 2.12) 64-Bit
- ALT SP Server 10 64-Bit
- ALT Server 10 64-Bit
- ALT 8 SP Server (LKNV.11100-01) 64-Bit
- ALT 8 SP Server (LKNV.11100-02) 64-Bit
- ALT 8 SP Server (LKNV.11100-03) 64-Bit
- Oracle Linux 7 64-Bit
- Oracle Linux 8 64-Bit
- Oracle Linux 9 64-Bit
- RED OS 7.3 Server 64-Bit
- RED OS 7.3 Certified Edition 64-Bit
- RED OS 8 Certified Edition 64-Bit
- ROSA COBALT 7.9 64-Bit

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

Die folgenden virtuellen Plattformen werden unterstützt:

- VMware vSphere 6.7.0
- VMware vSphere 7.0.3
- Citrix XenServer 7.x
- Citrix XenServer 8.2

- Parallels Desktop 18
- Oracle VM VirtualBox 7.0.12
- Kernel-basierte virtuelle Maschine (alle vom Administrationsserver unterstützten Linux-Betriebssysteme)

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

- MySQL 5.7 Community 32-Bit/64-Bit
- MySQL 8.0 32-Bit/64-Bit
- MariaDB 10.1 (Build 10.1.30 und höher) 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 10.5.17 und höher) 32-Bit/64-Bit
- MariaDB 10.6 (Build 10.6.9 und höher) 32-Bit/64-Bit
- MariaDB 10.11 (Build 10.11.3 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
- Postgres Pro 13.x 64-Bit (alle Editionen)
- Postgres Pro 14.x 64-Bit (alle Editionen)
- Postgres Pro 15.x 64-Bit (alle Editionen)
- Platform V Pangolin 5.4.0 64-Bit
- Jatoba 4 64-Bit

Anforderungen an die Web Console

Server der Kaspersky Security Center Web Console

Hardwaremindestvoraussetzungen:

- CPU: 4 Kerne, Taktfrequenz 2,5 GHz.
- RAM: 8 GB.

- Freier Speicherplatz auf dem Datenträger: 40 GB (/var/opt/kaspersky).

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

- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 12 (Bookworm)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 22.04 LTS (Jammy Jellyfish)
- CentOS Stream 9
- Red Hat Enterprise Linux Server 7.x
- Red Hat Enterprise Linux Server 8.x
- Red Hat Enterprise Linux Server 9.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.10015-37 (operatives Update 7.7)
- Astra Linux Common Edition (operatives Update 2.12)
- ALT SP Server 10
- ALT Server 10
- ALT 8 SP Server (LKNV.11100-01)
- ALT 8 SP Server (LKNV.11100-02)
- ALT 8 SP Server (LKNV.11100-03)
- Oracle Linux 7
- Oracle Linux 8
- Oracle Linux 9
- RED OS 7.3 Server

- RED OS 7.3 Certified Edition
- RED OS 8 Certified Edition
- ROSA COBALT 7.9
- Kernel-basierte virtuelle Maschine (alle vom Server der Kaspersky Security Center Web Console Server unterstützten Linux-Betriebssysteme)

Die folgenden virtuellen Plattformen werden unterstützt:

- VMware vSphere 6.7.0
- VMware vSphere 7.0.3
- Citrix XenServer 7.x
- Citrix XenServer 8.2
- Parallels Desktop 18
- Oracle VM VirtualBox 7.0.12
- Kernel-basierte virtuelle Maschine (alle vom Administrationsagenten unterstützten Linux-Betriebssysteme)

Client-Geräte

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

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 125.0.6422.76 oder höher (offizieller Build)
- Microsoft Edge 111.0.1661.41oder höher
- Safari 17.1 auf macOS
- Yandex.Browser 24.4.3.1012 oder höher
- Mozilla Firefox Extended Support Release 115.9.1 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 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 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) 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 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 2022 21H2 Standard/Datacenter 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 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

CentOS 6.7 und höher, 32-Bit

CentOS 6.x (bis 6.6) 32-Bit/64-Bit

CentOS 7.x 64-Bit

CentOS Stream 8 64-Bit

CentOS Stream 9 64-Bit

CentOS Stream 9 ARM 64-Bit

Red Hat Enterprise Linux Server 6.x 32-Bit/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

SUSE Linux Enterprise Server 12 (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 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 1.5) 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.10015-37 (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 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 Server 10 64-Bit

ALT Server 10 ARM 64-Bit

ALT Workstation 10 32-Bit/64-Bit

ALT 8 SP Workstation (8.4) ARM 64-Bit

ALT 8 SP Server (8.4) 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 Mageia 4 32-Bit Oracle Linux 7 64-Bit Oracle Linux 8 64-Bit Oracle Linux 9 64-Bit Linux Mint 20.x 64-Bit Linux Mint 21.1 und höher, 64-Bit AlterOS 7.5 und höher, 64-Bit GosLinux IC6/7.17 64-Bit GosLinux IC6/7.2 64-Bit SberOS 3.2.0 64-Bit Plattform V SberLinux OS Server (SLO) 8.8 64-Bit RED OS 7.3 ARM 64-Bit RED OS 7.3 Server 64-Bit RED OS 7.3 Certified Edition 64-Bit RED OS 8 Certified Edition 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 SynthesisM Server 8.6 64-bit SynthesisM Client 8.6 64-Bit OSnova 2.10 64-Bit Kylin 10 64-Bit EMIAS 1.0 64-Bit Amazon Linux 2 64-Bit MosOS 15.4 Arbat 64-Bit M OS (Moscow Electronic School) 64-Bit
Betriebssystem. macOS	macOS Monterey (12.x) macOS Ventura (13.x) macOS Sonoma (14.x) Für den Administrationsagenten werden außerdem sowohl die Architektur "Apple Silicon (M1)" als auch Intel unterstützt.
Virtualisierungsplattformen	VMware vSphere 6.7.0 VMware vSphere 7.0.3

	Citrix XenServer 7.x Citrix XenServer 8.2 Parallels Desktop 18 Oracle VM VirtualBox 7.0.12 Kernel-basierte virtuelle Maschine (alle vom Administrationsagenten unterstützten Linux-Betriebssysteme) Weitere Informationen finden Sie in den Anforderungen der verwalteten Anwendungen für andere unterstützte Plattformen.

Auf Geräten mit 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 von 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 gleichen Version wie zu installieren, wie Kaspersky Security Center Linux.

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 Programme und Lösungen von Kaspersky

Kaspersky Security Center Linux unterstützt die zentralisierte Bereitstellung und die Verwaltung der folgenden Programme und Lösungen von Kaspersky:

- Kaspersky Endpoint Security für Windows 12.0 oder höher (Unterstützung für Dateiserver)

- Kaspersky Endpoint Security für Linux 11.2 oder höher (Unterstützung für Dateiserver)
- Kaspersky Endpoint Security für Linux Elbrus Edition 10 oder höher
- Kaspersky Endpoint Security für Linux ARM Edition 11.2 oder höher
- Kaspersky Endpoint Security for Mac 11.3 oder höher
- Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 oder höher
- Kaspersky Industrial CyberSecurity for Nodes 3.2 oder höher
- Kaspersky Industrial CyberSecurity for Networks 3.2 oder höher
- Kaspersky Endpoint Agent 3.15 oder höher
- Kaspersky Embedded Systems Security für Windows 3.2 oder höher
- Kaspersky Embedded Systems Security für Linux 3.3 oder höher
- Kaspersky Security for Virtualization Light Agent 5.3 oder höher

Kaspersky Security Center Linux ist in den folgenden Lösungen enthalten:

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

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

Bekannte Probleme

Kaspersky Security Center Linux unterstützt die Verwaltung von Kaspersky Endpoint Security für Windows mit folgenden Einschränkungen: Die Komponenten von Kaspersky Sandbox werden nicht unterstützt.

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

Über die Kompatibilität von Administrationsserver und Kaspersky Security Center Web Console

Es wird empfohlen, sowohl den Kaspersky Security Center Linux Administrationsserver als auch die Kaspersky Security Center Web Console in der jeweils aktuellsten Version zu verwenden. Andernfalls wird möglicherweise die Funktionalität von Kaspersky Security Center Linux eingeschränkt.

Sie können den Kaspersky Security Center Linux Administrationsserver und die Kaspersky Security Center Web Console unabhängig voneinander installieren und aktualisieren. In diesem Fall sollten Sie sicherstellen, dass die Version der installierten Kaspersky Security Center Web Console mit der Version des Administrationsservers kompatibel ist, mit dem Sie eine Verbindung herstellen:

- Die in Kaspersky Security Center Linux 15.1 enthaltene Web Console unterstützt den Kaspersky Security Center Linux Administrationsserver in den folgenden Versionen: 15, 15.1, 14.2.

- Der in Kaspersky Security Center Linux 15.1 enthaltene Administrationsserver unterstützt die Kaspersky Security Center Web Console in den folgenden Versionen: 15, 15.1, 14.2.

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 Linux. 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.

Funktionsvergleich von Kaspersky Security Center als Windows-basierte Lösung und Linux-basierte Lösung

Funktion oder Eigenschaft	Kaspersky Security Center 14.2 Windows	Kaspersky Security Center 15.1 Linux
Standort des Administrationsservers	On-premises	On-premises
Standort des Datenbankmanagementsystems (DBMS)	On-premises	On-premises
Betriebssystem, auf dem der Administrationsserver installiert werden soll	Windows	Linux
Typ der Verwaltungskonsole	Lokal und webbasiert	Webbasiert
Betriebssystem, auf dem die webbasierte Verwaltungskonsole installiert werden soll	Windows oder Linux	Linux
Hierarchie des Administrationsservers	✓	✓
Hierarchie der Administrationsgruppen	✓	✓
Netzwerkabfrage	✓	✓
Maximale Anzahl verwalteter Geräte	100.000	50.000 (mit PostgreSQL und Postgres Pro)
Schutz von verwalteten Windows-, macOS- und Linux-verwalteten Geräten	✓	✓
Schutz von mobilen Geräten	✓	–
Schutz von virtuellen Maschinen	✓	✓
Schutz der Public-Cloud-Infrastruktur	✓	–
Gerätezentrierte Sicherheitsverwaltung	✓	✓
Benutzerzentrierte Sicherheitsverwaltung	✓	✓
Programmrichtlinien	✓	✓
Aufgaben für Kaspersky-Programme	✓	✓
Kaspersky Security Network	✓	✓
KSN-Proxy	✓	✓

Kaspersky Private Security Network	✓	✓
Zentralisierte Bereitstellung von Lizenzschlüsseln für Kaspersky-Programme	✓	✓
Automatisches Aktualisieren der Antiviren-Datenbanken	✓	✓
Unterstützung für virtuelle Administrationsserver	✓	✓
Installieren von Software-Updates von Drittanbietern und Beheben von Schwachstellen in Programmen von Drittanbietern	✓	✓
Benachrichtigungen über Ereignisse, die auf verwalteten Geräten auftreten	✓	✓
Erstellen und Verwalten von Benutzerkonten	✓	✓
Anmelden an der Konsole mit Domänenauthentifizierung	✓	✓ (Single Sign-On wird derzeit nicht unterstützt)
Integration von SIEM-Systemen	✓	✓ (nur mittels Syslog)
Statusüberwachung für Richtlinien und Aufgaben	✓	✓
Kaspersky Security Center Failover-Cluster bereitstellen	✓	✓
Installation des Administrationsservers in einem Windows Server Failover-Cluster	✓	–
Verwenden von SNMP, um Administrationsserver-Statistiken an Programme von Drittanbietern zu senden	✓	–
Ferndiagnose der Client-Geräte	✓	✓
Remote-Desktopverbindung mit einem Client-Gerät	✓	–
Umgang mit Objekt-Revisionen	✓	✓
Automatisches Aktualisieren der Kaspersky-Programme	✓	✓
Bereitstellen von Betriebssystemen auf Client-Geräten	✓	–
Webserver zum Veröffentlichen von Installationspaketen und anderen Dateien	✓	✓
Anzeigen und Bearbeiten der von Kaspersky Endpoint Detection and Response Optimum erkannte Alarme	✓	✓
Administrationsserver als WSUS-Server verwenden	✓	–
Integration mit Kaspersky Managed Detection and Response	✓	✓
Unterstützung der Adaptiven Kontrolle von Anomalien	✓	✓
Unterstützung von Clustern und Server-Arrays in Administrationsgruppen	✓	✓
Verwalten der Lizenzen von Drittanbietern	✓	–

Über die Kaspersky Security Center Cloud Console

Die Verwendung von Kaspersky Security Center als lokal installiertes Programm (on-premises) bedeutet, dass Sie Kaspersky Security Center inklusive Administrationsserver auf einem lokalen Gerät installieren, und die Netzwerksicherheit entweder durch die auf der Microsoft Management Console basierenden Verwaltungskonsole oder durch 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

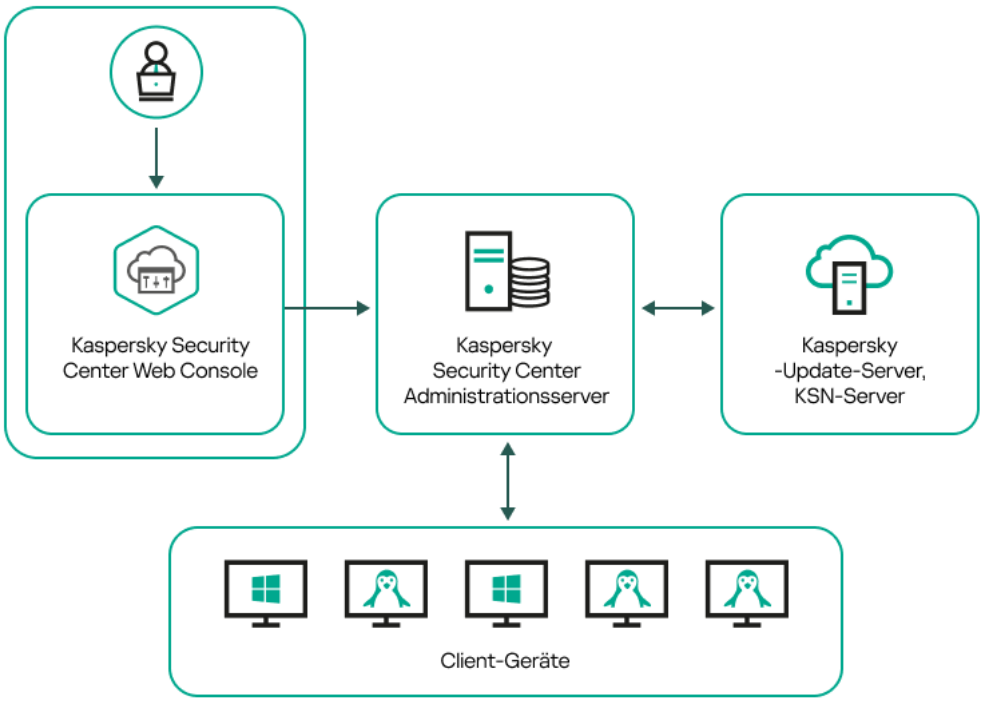
Weitere Informationen zu Kaspersky Security Center Cloud Console und seinen Funktionen finden Sie in der Dokumentation von Kaspersky Security Center Cloud Console und in der Dokumentation von Kaspersky Endpoint Security for Business.

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 Programme und deren Verwaltung aus.
- **Kaspersky-Update-Server**. HTTP(S)-Server bei Kaspersky, von denen Programme von Kaspersky Updates für Datenbanken und Programm-Module herunterladen.
- **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 Programme von Kaspersky auf Bedrohungen, erhöht die Leistungsfähigkeit einiger 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 Kaspersky-Sicherheits-Apps 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.

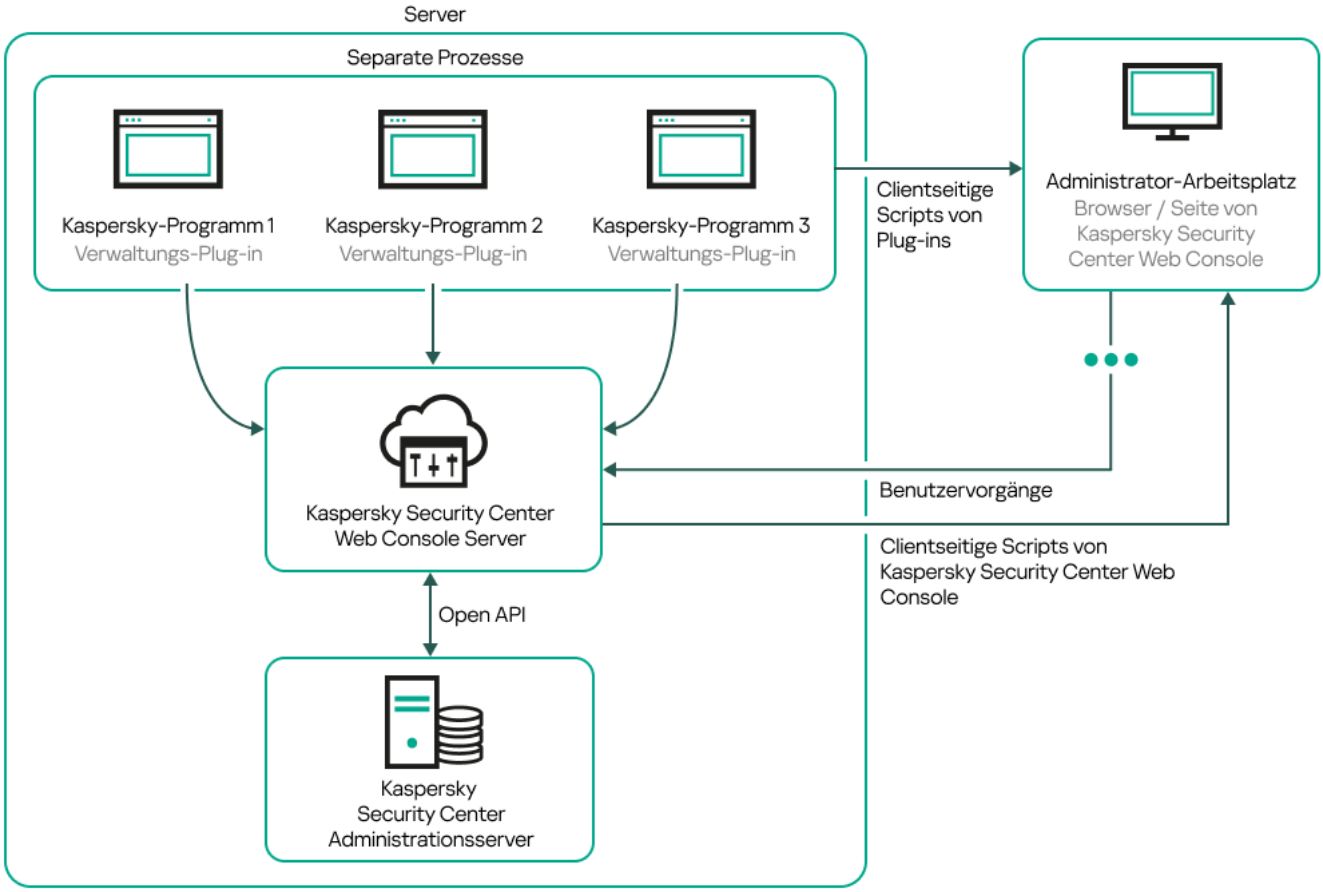


Diagramm der Softwareverteilung für Kaspersky Security Center Linux Administrationsserver und Kaspersky Security Center Web Console

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 Kaspersky Security Center Web Console 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 Kaspersky Security Center Web Console mit dem Kaspersky Security Center Linux Administrationsserver über OpenAPI. Der Server der Kaspersky Security Center Web Console 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 nachfolgenden Tabellen enthalten die standardmäßigen Ports, die auf dem Administrationsserver und auf den Client-Geräten geöffnet sein müssen. 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. Sie können die standardmäßige Portnummer im Abschnitt **Webserver** im Eigenschaftenfenster 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 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.
13299	klserver	TCP (TLS)	Aufbau von Verbindungen von der Kaspersky Security Center Web Console zum Administrationsserver; Aufbau von Verbindungen mit dem Administrationsserver über OpenAPI	Kaspersky Security Center Web Console, 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.
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.
13111 (nur,	ksnproxy	TCP	Annahme der Anfragen	KSN-Proxyserver.

wenn der KSN Proxy-Service auf dem Gerät ausgeführt wird)			von verwalteten Geräten an den 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.
17000	klactprx	TCP (TLS)	Annahme der Verbindungen zur Programmaktivierung 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**).
19170	klserver	HTTPS (TLS)	Tunneln der Verbindungen mit verwalteten Geräten mittels "klsctunnel"-Dienstprogramm	Remote-Verbindungen mit verwalteten Geräten mittels Kaspersky Security Center Web Console. Sie können die standardmäßige Portnummer mit dem Dienstprogramm klscflag ändern.

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 auf dem Server der Kaspersky Security Center Web Console geöffnet sein muss. 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 Kaspersky Security Center Web Console 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 zeigt den Port, der auf verwalteten Geräten mit installiertem Administrationsagent geöffnet sein muss.

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.

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 Programmen von Drittanbietern 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 zeigt die Ports, die auf einem verwalteten Gerät mit installiertem Administrationsagenten, welcher als Verteilungspunkt fungiert, geöffnet sein müssen. Die aufgelisteten Ports müssen auf den Verteilungspunkt-Geräten zusätzlich zu den von Administrationsagenten verwendeten Ports geöffnet sein (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	Verwaltung von Client-Geräten, Zustellung von

			und Verbindungs-Gateways empfangen	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.

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 Kaspersky Security Center Web Console (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	G
2001	KSCWebConsolePlugin	HTTPS	API-Port, der von den Prozessen der Verwaltungs-Plug-ins verwendet wird, um Anfragen des Dienstes KSCWebConsoleManagementService zu empfangen	A K P V P
1329, 2003	KSCWebConsoleManagementService	HTTPS	API-Ports, die verwendet werden, um Anfragen von dem auf dem gleichen Gerät ausgeführten Dienst "KSCWebConsole" zu empfangen	A K K S W
2005	KSCWebConsole	HTTPS	API-Port, der verwendet wird, um Anfragen von dem auf dem gleichen Gerät ausgeführten KSCWebConsoleManagementService-Dienst zu empfangen	A K P K S W
8200	—	HTTP	API-Port, der für die Erstellung von Zertifikaten unter Verwendung von HashiCorp Vault verwendet wird	In K S W

			(Weitere Informationen entnehmen Sie der Website von HashiCorp Vault)	A K K S W
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	API-Ports des Message Brokers, die für die Kommunikation zwischen den Prozessen von Kaspersky Security Center Web Console und den Verwaltungs-Plug-ins verwendet werden	In z K S W V P

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-Programme.

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 Programmpakete
- Remote-Installation von Programmen auf Client-Geräten und Löschen von Programmen
- Datenbanken-Update und Update der Programm-Module von Kaspersky
- 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-Programmen
- 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 Programmoberfläche

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 mir 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 das Programm 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 Backup 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-Programmen 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://<Webservername>:<HTTPS-Port>/public/<Objekt>
```

wobei:

- `<Webservername>` 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 `<Objekt>` 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.

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-Programme mit Kaspersky Security Center Linux verwaltet werden.

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

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

Ein Gerät, auf dem der Administrationsagent installiert ist, wird als *verwaltetes Gerät* oder *Gerät* bezeichnet. Den Administrationsagenten können Sie aus einer der folgenden Quellen installieren:

- Installationspaket im Speicher des Administrationsservers (dazu müssen Sie den Administrationsserver installiert haben)
- Installationspaket, das sich auf den Kaspersky-Webservern befindet

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.

Die Namen des Prozesses, den der Administrationsagent startet, lauten wir folgt:

- klnagent64.service (für 64-Bit-Betriebssysteme)
- klnagent.service (für 32-Bit-Betriebssysteme)

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 Programmeinstellungen (die Sie in Gruppenrichtlinien festlegen können).
- Verwenden eines allgemeinen Betriebsmodus für alle Programme, indem Gruppenaufgaben mit festgelegten Einstellungen erstellt werden. Beispiele für Gruppenaufgaben umfassen unter anderem das Erstellen und Installieren eines Standard-Installationspakets, Aktualisieren von Programm-Datenbanken und Modulen, 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 den Computer dieses Mitarbeiters von der Administrationsgruppe "Buchhalter" in die Administrationsgruppe "Entwickler" verschieben. Danach erhält der Computer automatisch die Programmeinstellungen, die für Entwickler erforderlich sind.

Verwaltetes Gerät

Ein *verwaltetes Gerät* ist ein Computer, 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. Ein Administrationsserver kann bis zu 20.000 Geräte verwalten.

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 Programme 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 Kaspersky Security Center Web Console 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-Programme 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 einem spezifischen Programm von Kaspersky. Mit einem Verwaltungs-Plug-in können Sie Aufgaben und Richtlinien für die Anwendung konfigurieren.

Sie können die Web-Plug-ins zur Verwaltung von der Webseite des Technischen Supports von Kaspersky 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-Programmen 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 Kaspersky-Programmeinstellungen, die auf eine Administrationsgruppe und deren Untergruppen angewendet werden. Sie können mehrere Kaspersky-Programme auf den Geräten einer Administrationsgruppe installieren. Kaspersky Security Center bietet eine einzelne Richtlinie für jedes Kaspersky-Programm 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 ein Kaspersky-Programm aktiv sein. Geräte wenden die Einstellungswerte einer aktiven Richtlinie für ein Kaspersky-Programm 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 ein einzelnes Programm können mehrere Richtlinien mit unterschiedlichen Werten konfiguriert werden.
- Für das aktuelle Programm 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 lokale Programmeinstellungen 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 Programmen, Untersuchung von Dateien, Datenbanken-Update und Aktualisierung der Programm-Module sowie Ausführung anderer Aktionen mit den Programmen.

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
- Installationspaket anhand des Betriebssystem-Abbilds eines Mustergeräts erstellen

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-App). 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 jedes Programm 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 das Programm 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 der Satz 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.

- 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 Datenbank des Administrationsservers eingegeben wurden. Darüber hinaus müssen die Informationen entweder während einer bestehenden Verbindung der Geräte oder während einer Gerätesuche eingegeben worden sein.

- Geräteauswahl festlegen.

  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 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 eines Programms für alle Geräte gesetzt werden, die zu einer Gruppe gehören.

Die Einstellungswerte, die eine Richtlinie vorgibt, lassen sich für einzelne Geräte mit lokalen Programmeinstellungen 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 das Programm 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 das Programm den lokalen Einstellungswert auf jedem Client-Gerät und nicht den Wert, der in der Richtlinie angegeben ist. Der Einstellungswert kann dabei über die lokalen Programmeinstellungen geändert werden.

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

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

- Durch die Gruppenrichtlinie, wenn die Änderung der Einstellung gesperrt wurde.

Die lokalen Programmeinstellungen 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 Programmen und den Empfang von Informationen über Geräte im Netzwerk. 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-Programmen und von Programmen 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 Programmversionen 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 klnagchk-Bericht 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.

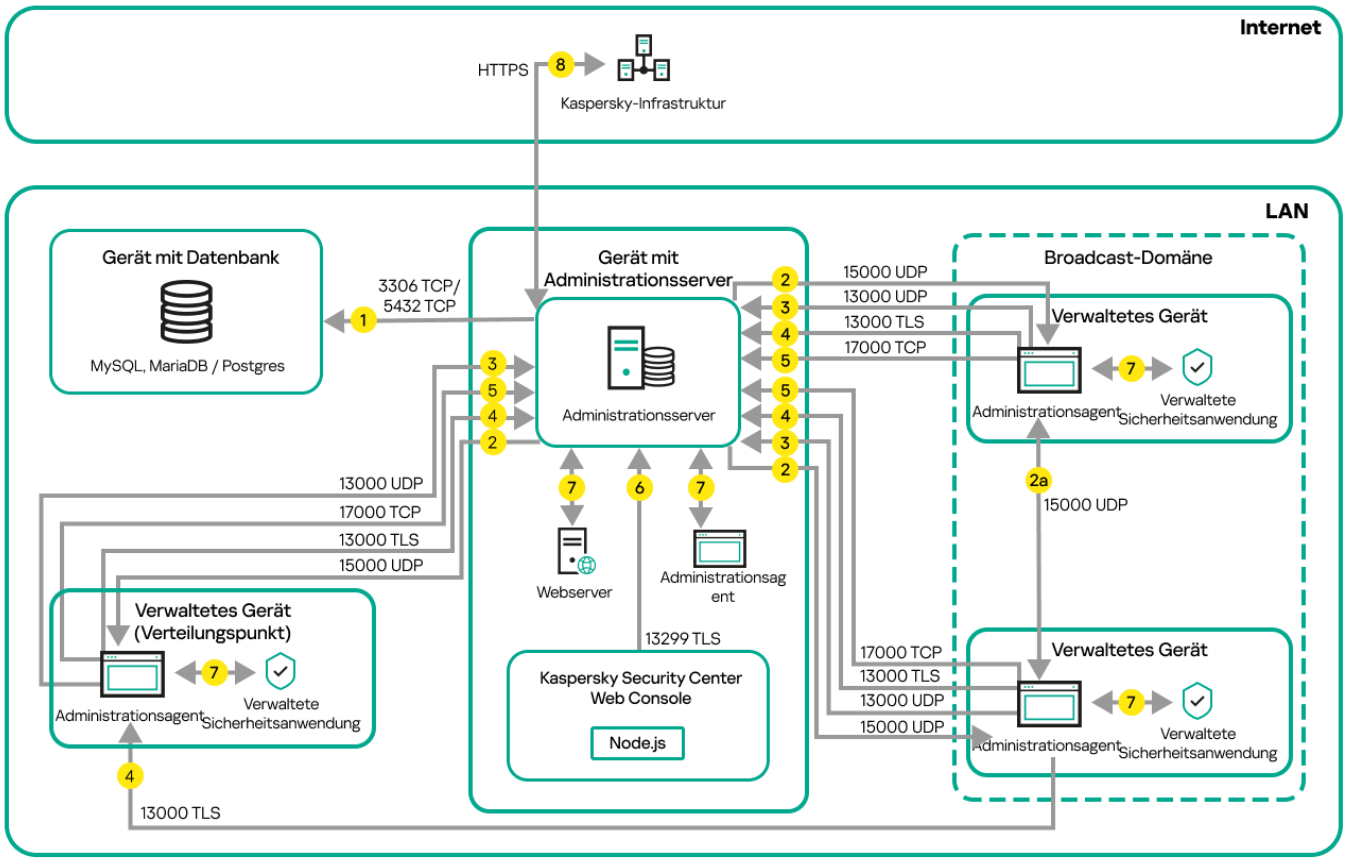
- Sie können Verbindungs-Gateways auch innerhalb des Netzwerks verwenden. Beispielsweise werden automatisch zugewiesene Verteilungspunkte auch zu Verbindungs-Gateways in ihrem eigenen Bereich. Innerhalb eines internen Netzwerks bieten Verbindungs-Gateways jedoch keinen wesentlichen Vorteil. Sie reduzieren 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.

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 SSL-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-SSL-Port 14000 annehmen. Kaspersky Security Center unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den SSL-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 Kaspersky Security Center Web Console sendet über den TLS-Port 13299 Daten an den Administrationsserver, der auf demselben oder auf einem anderen Gerät installiert sein kann.

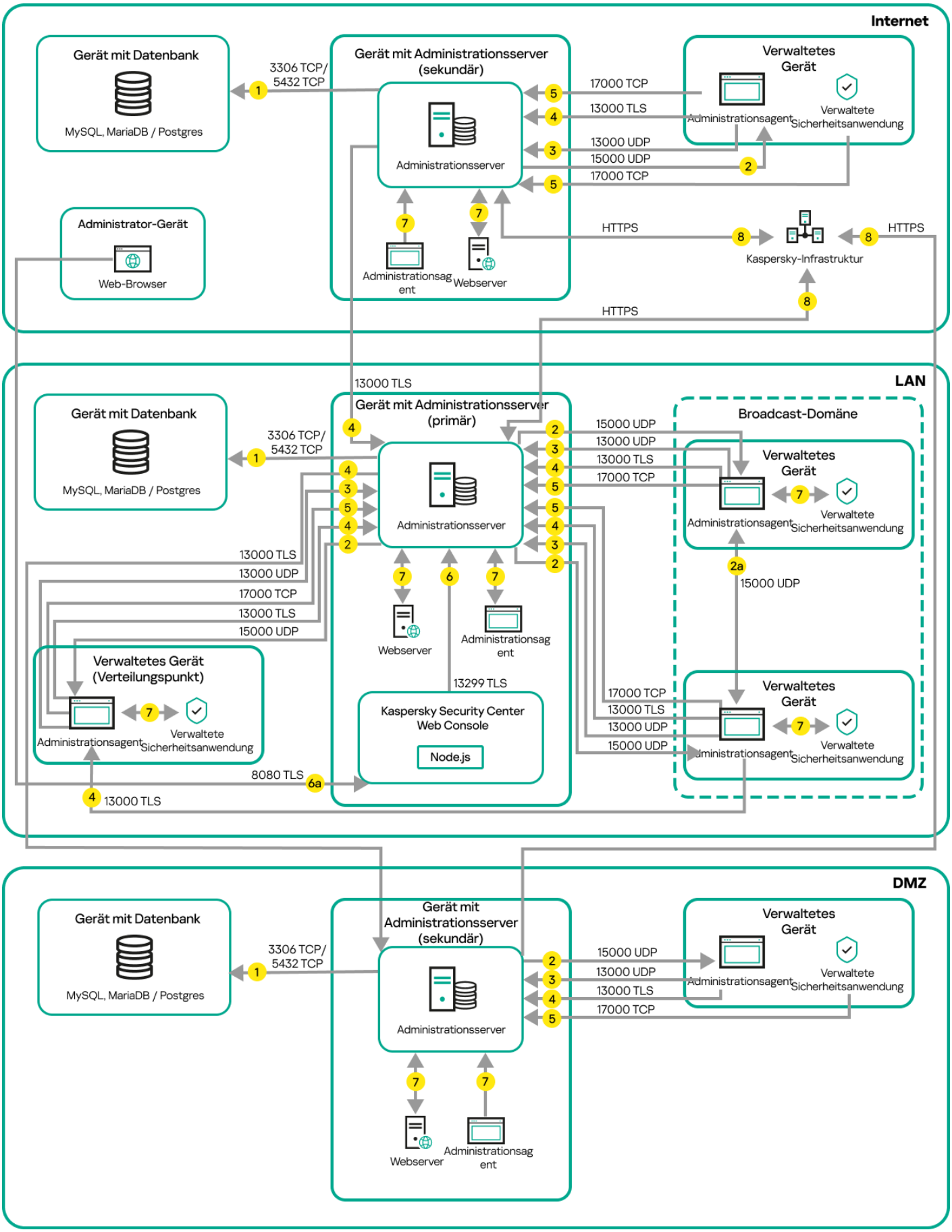
7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

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.

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 SSL-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-SSL-Port 14000 annehmen. Kaspersky Security Center Linux unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den SSL-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 Kaspersky Security Center Web Console 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 Kaspersky Security Center Web Console übermittelt. Der Server der Kaspersky Security Center Web Console kann entweder auf dem Administrationsserver oder auf einem anderen Gerät installiert werden.

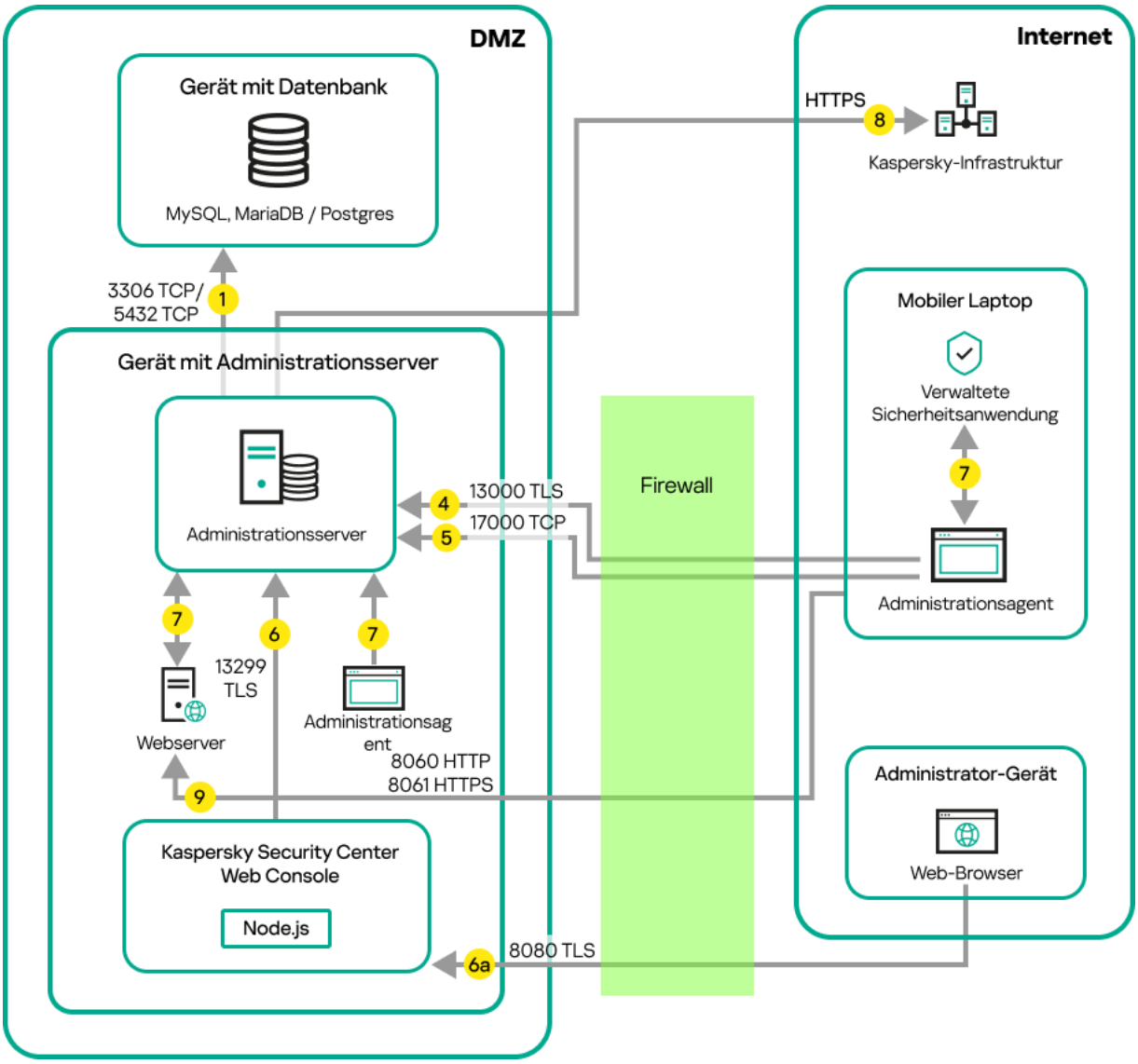
7. Die Programme auf einem einzelnen Gerät tauschen lokalen Datenverkehr aus (auf dem Administrationsserver oder auf einem verwalteten Gerät). Es müssen keine externen Ports geöffnet werden.

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.

Administrationsserver im LAN, verwaltete Geräte im Internet und Verwendung einer Firewall

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 eine beliebige Unternehmens-Firewall verwendet. Weitere Einzelheiten entnehmen Sie der Dokumentation dieser Anwendung.



Administrationsserver im lokalen Netzwerk; verwaltete Geräte stellen über eine Unternehmens-Firewall 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 SSL-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-SSL-Port 14000 annehmen. Kaspersky Security Center Linux unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den SSL-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 Kaspersky Security Center Web Console 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 Kaspersky Security Center Web Console übermittelt. Der Server der Kaspersky Security Center Web Console 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.

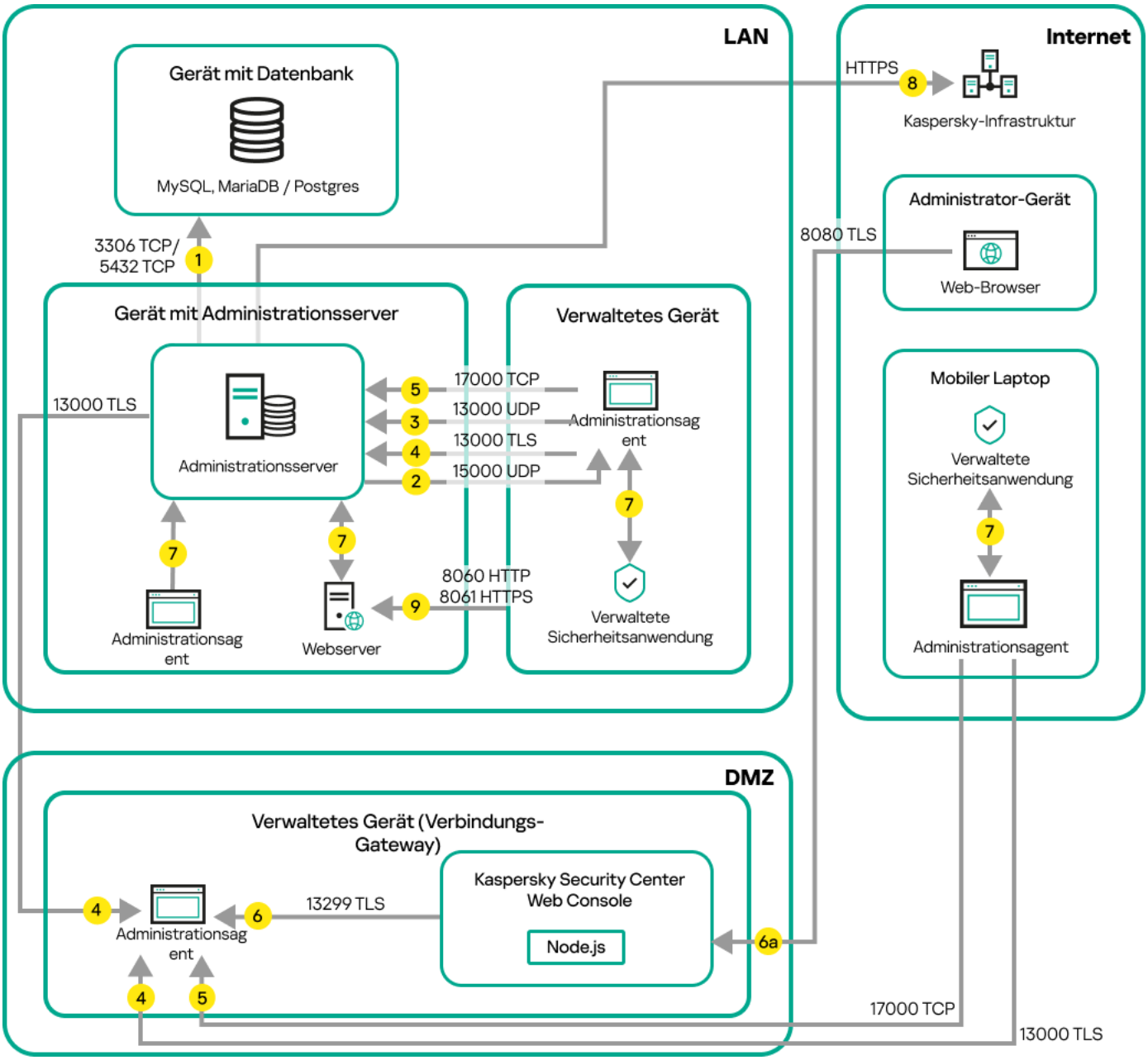
   Wenn Sie nicht möchten, dass Ihr Administrationsserver Zugang zum Internet hat, müssen Sie diese Daten manuell verwalten.

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

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 ein Microsoft Forefront Threat Management Gateway (TMG) noch eine Unternehmens-Firewall nutzen möchten.



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 TMG 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, 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 SSL-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-SSL-Port 14000 annehmen. Kaspersky Security Center Linux unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den SSL-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 Kaspersky Security Center Web Console 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 Kaspersky Security Center Web Console übermittelt. Der Server der Kaspersky Security Center Web Console 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.

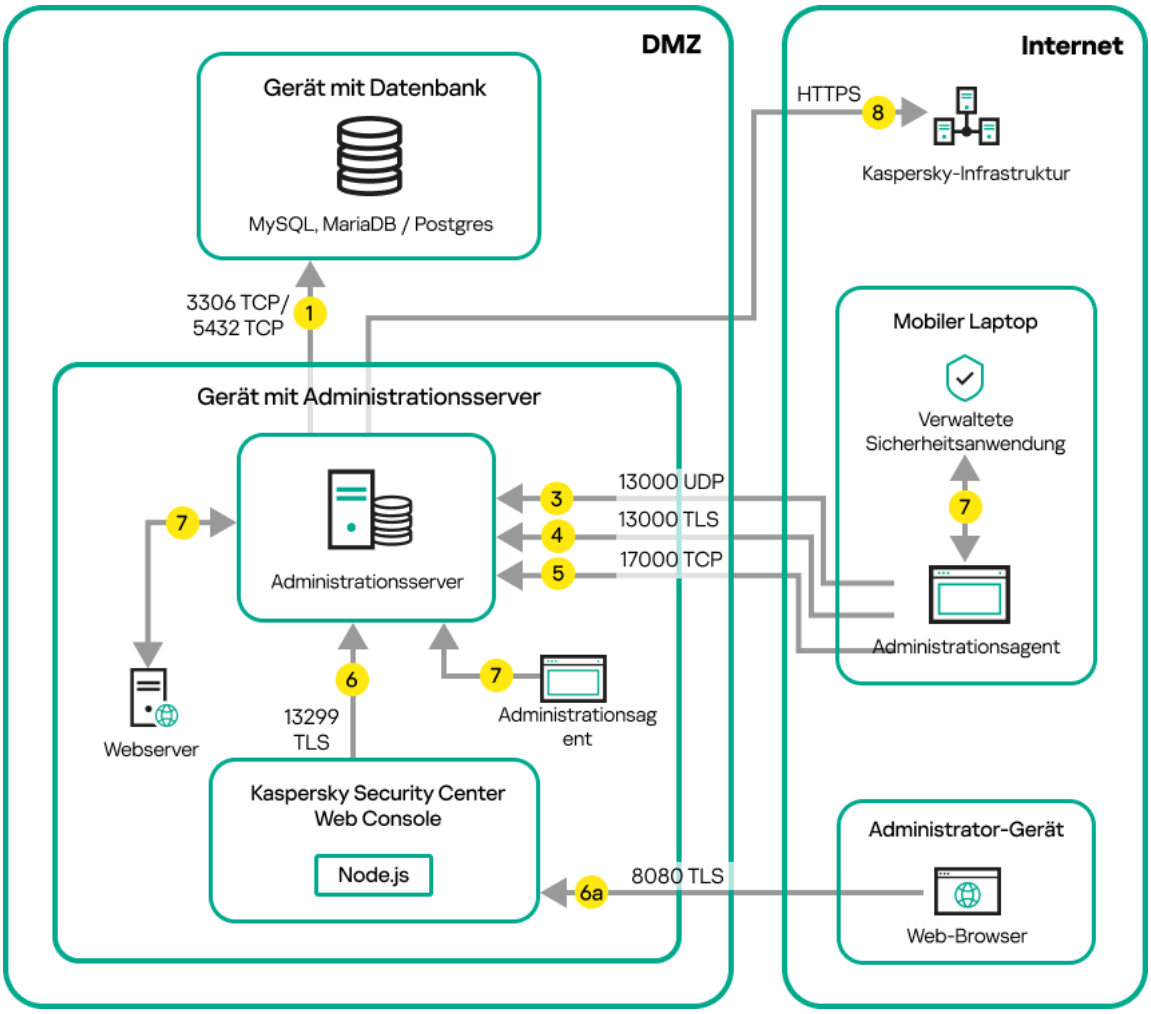
8. Die Daten vom Administrationsserver an die Kaspersky-Server (z. B. KSN-Daten oder Lizenzinformationen) sowie die Daten von den Kaspersky-Servern zum Administrationsserver (z. B. Programm-Updates oder Updates der Antiviren-Datenbanken) werden via HTTPS-Protokoll übertragen.

   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.

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 SSL-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-SSL-Port 14000 annehmen. Kaspersky Security Center Linux unterstützt zwar auch die Verbindung von Administrationsagenten über Port 14000, aber es wird empfohlen, den SSL-Port 13000 zu verwenden.

   4a. Ein in der DMZ vorhandenes Verbindungs-Gateway empfängt ebenfalls Verbindungen vom Administrationsserver über den SSL-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 SSL-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 Kaspersky Security Center Web Console 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 Kaspersky Security Center Web Console übermittelt. Der Server der Kaspersky Security Center Web Console 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.

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.

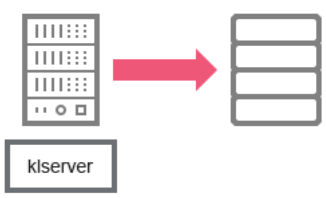
Konventionen für die Interaktionsschemata

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

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 werden in die Datenbank aufgenommen.

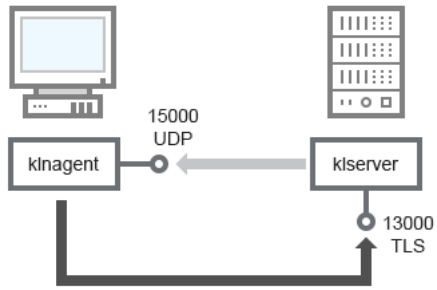


Administrationsserver und DBMS

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). Relevante Informationen finden Sie in der DBMS-Dokumentation.

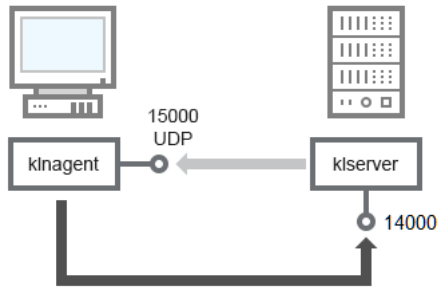
Administrationsserver und Client-Gerät: Verwaltung der Sicherheitsanwendung

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)

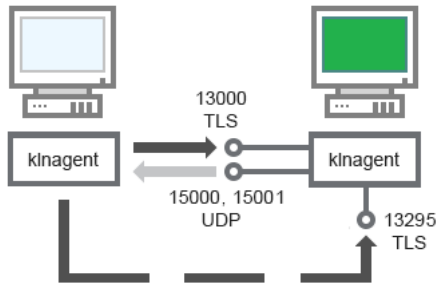
Erklärungen zum Schema finden Sie in den nachfolgenden Tabellen.

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-Upgrades auf dem Client-Gerät mithilfe des Verteilungspunkts

Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

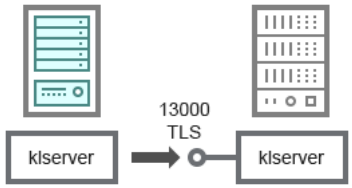
Software-Upgrades mithilfe des Verteilungspunkts (Datenverkehr)

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.

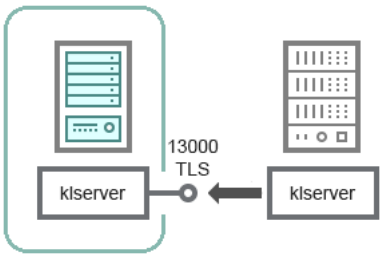


Erklärungen zum Schema finden Sie in der nachfolgenden Tabelle.

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

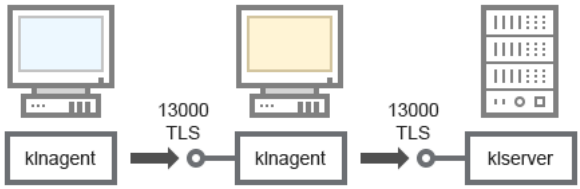
Das Schema zeigt die Hierarchie der Administrationsserver, in welcher der sekundäre Administrationsserver, der sich in der demilitarisierten Zone befindet, die Verbindung vom primären Administrationsserver übernimmt (eine Erklärung zum Schema finden Sie in der nachstehenden Tabelle). Bei der Zusammenfassung 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



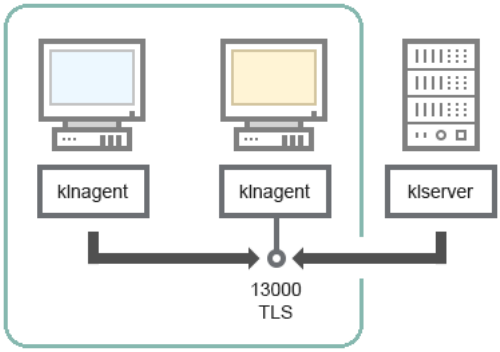
Administrationsserver, Verbindungs-Gateway im Netzwerksegment und Client-Gerät

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



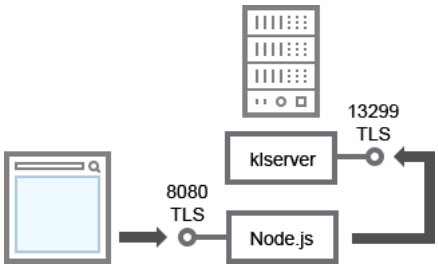
Administrationsserver Verbindungs-Gateway und Client-Gerät in der demilitarisierten Zone

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)	Aufbau von Verbindungen von der Kaspersky Security Center Web Console mit dem Administrationsserver über OpenAPI
Server oder Administrationsserver der Kaspersky Security Center Web Console	8080	Node.js: Serverseitiges JavaScript	TCP (TLS)	Empfangen von Verbindungen von Kaspersky Security Center Web Console

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-Apps auf den verwalteten Geräten installieren.

Erforderliche Vorrausetzungen

Sie müssen einen Lizenzschlüssel (Aktivierungscode) für Kaspersky Endpoint Security for Business oder Lizenzschlüssel (Aktivierungscodes) für Kaspersky-Sicherheits-Apps 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 die Büros verteilt werden müssen, wenn Sie mit einem verteilten Netzwerk arbeiten.

   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. Die Daten können dabei teilweise und auf manuelle Weise in eine andere Datenbank übertragen werden.

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 das Programm 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 Apps von Kaspersky und 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 Programmen, 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 Programmeinstellungen 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.

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

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=<Wert>
   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
   ```

   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.

   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.

PostgreSQL- oder Postgres Pro-Server für die Ausführung mit Kaspersky Security Center Linux konfigurieren

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`

Empfohlene Parameter für PostgreSQL und Postgres Pro:

- `shared_buffers` = 25% der Arbeitsspeichergröße des Geräts, auf dem das DBMS installiert ist

  Wenn der Arbeitsspeicher weniger als 1 GB beträgt, belassen Sie den Standardwert.
- `max_stack_depth` = maximale Stapelgröße (führen Sie den Befehl `ulimit -s` aus, um diesen Wert in KB zu erhalten) minus 1 MB Sicherheitsdifferenz
- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `max_connections=151`
- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128 MB`

Um nach einer Aktualisierung der Datei "postgresql.conf" die Änderungen zu übernehmen, starten oder laden Sie den Server neu. Weitere Informationen entnehmen Sie in der offiziellen Dokumentation von PostgreSQL.

Weitere Informationen zum Erstellen und Konfigurieren von Konten für PostgreSQL und Postgres Pro finden Sie im folgenden Thema: Benutzerkonten für die Arbeit mit PostgreSQL und Postgres Pro konfigurieren.

Weitere Informationen zu den Serverparametern von PostgreSQL und Postgres Pro und zu deren Konfiguration finden Sie in der entsprechenden DBMS-Dokumentation.

Kaspersky Security Center Linux installieren

In diesem Ablauf wird beschrieben, wie Kaspersky Security Center Linux installiert wird.

Vor der Installation:

- Installieren Sie ein DBMS.

- Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center Linux installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

Verwenden Sie die Installationsdatei ksc64_[Versionsnummer]_amd64.deb oder ksc64-[Versionsnummer].x86_64.rpm, die der auf Ihrem Gerät installierten Linux-Distribution entspricht. Sie erhalten die Installationsdatei, indem Sie diese von der Kaspersky-Website herunterladen.

Um Kaspersky Security Center Linux zu installieren, führen Sie die in den folgenden Schritten angegebenen Befehle unter einem Benutzerkonto mit Root-Rechten aus.

So installieren Sie Kaspersky Security Center Linux:

1. Wenn Ihr Gerät unter Astra Linux 1.8 oder höher läuft, führen Sie die in diesem Schritt beschriebenen Aktionen aus. Wenn Ihr Gerät unter einem anderen Betriebssystem läuft, fahren Sie mit dem nächsten Schritt fort.

   a. Erstellen Sie das Verzeichnis "/etc/systemd/system/kladminserver_srv.service.d" und legen Sie die Datei "override.conf" mit folgendem Inhalt an:
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Erstellen Sie das Verzeichnis "/etc/systemd/system/klwebsrv_srv.service.d" und legen Sie die Datei "override.conf" mit folgendem Inhalt an:
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

2. Erstellen Sie die Gruppe "kladmins" und das nicht privilegierte Benutzerkonto "ksc". 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
   ```

3. Führen Sie die Installation von Kaspersky Security Center Linux aus. Führen Sie abhängig von Ihrer Linux-Distribution einen der folgenden Befehle aus:

   - `# apt install /<path>/ksc64_[Versionsnummer]_amd64.deb`
   - `# yum install /<path>/ksc64-[Versionsnummer].x86_64.rpm -y`

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. Geben Sie nach der entsprechenden Aufforderung die folgenden Einstellungen ein:

a. Geben Sie den DNS-Namen oder die statische IP-Adresse des Administrationsservers ein (`127.0.0.1` für eine lokale DB-Installation)

b. Geben Sie die SSL-Portnummer des Administrationsservers ein. Standardmäßig ist die Portnummer 13000 festgelegt.

c. Ermitteln Sie die ungefähre Anzahl der Geräte, die Sie verwalten möchten:

- Geben Sie für 1 bis 100 vernetzte Geräte den Wert 1 ein.
- Geben Sie für 101 bis 1.000 vernetzte Geräte den Wert 2 ein.
- Geben Sie für über 1.000 vernetzte Geräte den Wert 3 ein.

d. Geben Sie den Namen der Sicherheitsgruppe für Dienste ein. Standardmäßig wird die Gruppe `kladmins` verwendet.

e. 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.

f. 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.

g. 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.

h. Geben Sie den DNS-Namen oder die IP-Adresse des Gerätes ein, auf dem die Datenbank installiert ist (`127.0.0.1` für eine lokale DB-Installation).

i. 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

j. Geben Sie den Namen der Datenbank ein.

k. Geben Sie den Benutzernamen des Datenbank-Root-Benutzerkontos ein, das Sie für den Zugriff auf die Datenbank verwenden.

l. Geben Sie das Kennwort des Datenbank-Root-Benutzerkontos ein, das Sie für den Zugriff auf die Datenbank verwenden.

Warten Sie, bis die Dienste hinzugefügt und automatisch gestartet wurden:

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. Erstellen Sie ein Benutzerkonto, das als Administrator des Administrationsservers fungiert. Geben Sie den Benutzernamen und das Kennwort ein. Mit dem folgenden Befehl können Sie einen neuen Benutzer erstellen: `/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <Kennwort>`

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

Der Benutzer wird hinzugefügt und Kaspersky Security Center Linux wird installiert.

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`

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 benutzerdefinierten Zusammenstellung von Installationsparametern: Variablen und ihre entsprechenden Werte.

Vor der Installation:

- Installation eines Datenbank-Managementsystems (DBMS).

- Stellen Sie sicher, dass auf dem Gerät, auf dem Sie Kaspersky Security Center Linux installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

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. Wenn Ihr Gerät unter Astra Linux 1.8 oder höher läuft, führen Sie die in diesem Schritt beschriebenen Aktionen aus. Wenn Ihr Gerät unter einem anderen Betriebssystem läuft, fahren Sie mit dem nächsten Schritt fort.

   a. Erstellen Sie das Verzeichnis "/etc/systemd/system/kladminserver_srv.service.d" und legen Sie die Datei "override.conf" mit folgendem Inhalt an:
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Erstellen Sie das Verzeichnis "/etc/systemd/system/klwebsrv_srv.service.d" und legen Sie die Datei "override.conf" mit folgendem Inhalt an:
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

3. Erstellen Sie eine Gruppe "kladmins" und ein nicht privilegiertes Benutzerkonto "ksc", welches zwingend ein Mitglied der Gruppe "kladmins" ist. 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
   ```

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 separaten Zeile. Die Antwortdatei sollte die Variablen enthalten, die in der folgenden Tabelle aufgeführt sind.

5. Geben Sie in der Root-Umgebung 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:

   - `# apt install /<path>/ksc64_[Versionsnummer]_amd64.deb`
   - `# 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 ksc -p <Kennwort>`, wobei das Kennwort mindestens 8 Zeichen enthalten muss.

Name der Variablen	Notwendig	Beschreibung	Möglic
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 Adresse
KLSRV_UNATT_PORT_SRV	Nein	Die Portnummer des Administrationsservers. Optional. Standardwert ist 14000.	Portnumme
KLSRV_UNATT_PORT_SRV_SSL	Nein	Die SSL-Portnummer des Administrationsservers. Optional. Standardwert ist 13000.	Portnumme
KLSRV_UNATT_PORT_KLOAPI	Nein	Die KLOAPI-Portnummer des Administrationsservers. Optional. Standardwert ist 13299.	Portnumme
KLSRV_UNATT_PORT_GUI	Nein	Die Portnummer für die Benutzeroberfläche des Administrationsservers. Optional. Standardwert ist 13291.	Portnumme
KLSRV_UNATT_NETRANGETYPE	Nein	Die ungefähre Anzahl an Geräten, die Sie verwalten möchten: Optional. Standardwert ist 1.	1 für 1 bis 1C Geräte. 2 für 101 bis vernetzte G 3 für mehr a vernetzte G
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.	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.	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_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 des Administrationsservers als Kaspersky Security Center Linux Failover-Cluster, muss Antwortdatei die folgenden zusätzlichen Variablen enthalten:			
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.	VirtualAd oder ExternalL
Falls die Variable KLFOC_UNATT_CONN_MODE den Wert VirtualAdapter besitzt, muss die Antwortdatei die 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-Adress

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 Programmschlüssel kaspersky_astra_pub_key.gpg herunter.

Verwenden Sie die Installationsdatei ksc64_[Versionsnummer]_amd64.deb. Sie erhalten die Installationsdatei, indem Sie diese von der Kaspersky-Website herunterladen.

> 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_initrafs.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 Programmschlüssel:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Legen Sie den Programmschlüssel 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. Wenn Ihr Gerät unter Astra Linux 1.8 oder höher läuft, führen Sie die in diesem Schritt beschriebenen Aktionen aus. Wenn Ihr Gerät unter einem anderen Betriebssystem läuft, fahren Sie mit dem nächsten Schritt fort.

   a. Erstellen Sie das Verzeichnis "/etc/systemd/system/kladminserver_srv.service.d" und legen Sie die Datei "override.conf" mit folgendem Inhalt an:

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Erstellen Sie das Verzeichnis "/etc/systemd/system/klwebsrv_srv.service.d" und legen Sie die Datei "override.conf" mit folgendem Inhalt an:

   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

7. Erstellen Sie die Gruppe "kladmins" und das nicht privilegierte Benutzerkonto "ksc". 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
   ```

8. Starten Sie die Installation von Kaspersky Security Center Linux:
   ```
   # apt install /<path>/ksc64_[Versionsnummer]_amd64.deb
   ```

9. Führen Sie die Konfiguration von Kaspersky Security Center Linux aus:
   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

10. 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.

11. 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 vernetzte Geräte den Wert 1 ein.
    - Geben Sie für 101 bis 1.000 vernetzte Geräte den Wert 2 ein.
    - Geben Sie für über 1.000 vernetzte Geräte den Wert 3 ein.

    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. Geben Sie die IP-Adresse des Gerätes ein, auf dem die Datenbank installiert ist.

i. Geben Sie die Portnummer der Datenbank ein. Dieser Port wird für die Kommunikation mit dem Administrationsserver verwendet. Standardmäßig ist die Portnummer 3306 festgelegt.

j. Geben Sie den Namen der Datenbank ein.

k. Geben Sie den Benutzernamen des Datenbank-Root-Benutzerkontos ein, das Sie für den Zugriff auf die Datenbank verwenden.

l. Geben Sie das Kennwort des Datenbank-Root-Benutzerkontos ein, das Sie für den Zugriff auf die Datenbank verwenden.

Warten Sie, bis die Dienste hinzugefügt und automatisch gestartet wurden:

- `klnagent_srv`
- `kladminserver_srv`
- `klactprx_srv`
- `klwebsrv_srv`

m. 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 Gruppen enthalten:
  - Großbuchstaben (A–Z)
  - Kleinbuchstaben (a–z)
  - Zahlen (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`

Kaspersky Security Center Web Console installieren

In diesem Abschnitt wird beschrieben, wie Sie den Server der Kaspersky Security Center Web Console (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, die der auf Ihrem Gerät installierten Linux-Distribution entspricht:

- Für Debian – ksc-web-console-[Build-Nummer].x86_64.deb
- Für RPM-basierte Betriebssysteme – ksc-web-console-[Build-Nummer].x86_64.rpm
- Für ALT 8 SP – ksc-web-console-[Build-Nummer]-alt8p.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. Nennen Sie die Datei "ksc-web-console-setup.json" und platzieren Sie diese in dem folgenden Pfad: /etc/ksc-web-console-setup.json.

   Beispiel für eine Antwortdatei mit minimalem Parametersatz sowie Standardadresse und Standardport:

   ```
   {
     "address": "127.0.0.1",
     "port": "8080",
     "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
     "acceptEula": "true"
   }
   ```

   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 dpkg -i 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 rpm -ivh --nodeps 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 rpm -Uvh --nodeps --force ksc-web-console-[Build-Nummer].x86_64.rpm
    ```
  - Für Geräte mit Debian-basiertem Betriebssystem:
    ```
    $ sudo dpkg -i 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.

Installationsparameter für Kaspersky Security Center Web Console

Für die Installation von Server der Kaspersky Security Center Web Console 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.

Hier ist ein Beispiel für eine Antwortdatei mit dem minimalem Parametersatz sowie Standardadresse und Standardport:

```
{
  "address": "127.0.0.1",
  "port": "8080",
  "defaultLangId": 1049,
  "enableLog": false,
 "trusted": "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
Server",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
  "webConsoleAccount": "Group1:User1",
"managementServiceAccount": "Gruppe1:Benutzer2",
"serviceWebConsoleAccount": "Gruppe1:Benutzer3",
"pluginAccount": "Gruppe1:Benutzer4",
"messageQueueAccount": "Group1:User5"
}
```

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 Wert
`Adresse`	Adresse des Servers der Kaspersky Security Center Web Console (erforderlich).	Zeichenfolgenwert.
`Port`	Nummer des Ports, über den der Server der Kaspersky Security Center Web Console eine Verbindung zum Administrationsserver herstellt (erforderlich).	Zahlenwert.
`defaultLangId`	Sprache der Benutzeroberfläche (standardmäßig `1033`).	Zahlencodes der Sprachen: • Deutsch: `1031` • Englisch: `1033` • Spanisch: `3082` • Spanisch (Mexiko): `2058` • Französisch: `1036` • Japanisch: `1041` • Kasachisch: `1087` • Polnisch: `1045` • Portugiesisch (Brasilien): `1046` • Russisch: `1049` • Türkisch: `1055` • Vereinfachtes Chinesisch: `4` • Traditionelles Chinesisch: `31748` Wenn kein Wert angegeben ist, wird Engli
`enableLog`	Gibt an, ob die Aktivitätsprotokollierung in Kaspersky Security Center Web Console aktiviert werden soll oder nicht.	Boolescher Wert: • `true` – Protokollierung aktiviert (stand • `false` – Protokollierung deaktiviert.
`Vertrauenswürdig`	Liste der vertrauenswürdigen	Zeichenkette im folgenden Format:

	Administrationsserver, die zur Verbindung mit Kaspersky Security Center Web Console berechtigt sind. Für jeden Administrationsserver müssen die folgenden Parameter definiert sein: • Adresse des Administrationsservers • OpenAPI-Port, der von Kaspersky Security Center Web Console zur Verbindung mit dem Administrationsserver genutzt wird (standardmäßig 13299) • Pfad zum Zertifikat des Administrationsservers • Der im Login-Fenster anzuzeigende Name des Administrationsservers Die Parameter werden durch senkrechte Striche separiert. Wenn mehrere Administrationsserver angegebenen werden, separieren Sie diese durch zwei senkrechte Striche (Pipes).	`"Serveradresse|Port|Pfad des Zertifikats|Servername"`. Beispiel: `"X.X.X.X|13299|/cert/server-1.ce 1||Y.Y.Y.Y|13299|/cert/server-2.`
`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 habe die Bedingungen des Lizenzvertrags vollständig gelesen, un sie. • `false` – Ich akzeptiere die Bedingung Lizenzvertrags nicht (standardmäßig a Wenn kein Wert angegeben ist, zeigt Ihne der Kaspersky Security Center Web Cons nach, ob Sie den Bedingungen der EULA z
`certDomain`	Wenn Sie ein neues Zertifikat generieren möchten, können Sie mithilfe dieses Parameters den Domänennamen angeben, für den das Zertifikat generiert werden soll.	Zeichenfolgenwert.
`certPath`	Wenn Sie ein bestehendes Zertifikat verwenden möchten, können Sie mithilfe dieses Parameters den Pfad zur Zertifikatsdatei angeben.	Zeichenfolgenwert. Geben Sie den Pfad `/var/opt/kaspersky/klnagent_srv/` an, um das vorhandene Zertifikat zu verwe benutzerdefiniertes Zertifikat den Speich benutzerdefinierten Zertifikats an.

`keyPath`	Wenn Sie ein bestehendes Zertifikat verwenden möchten, können Sie mithilfe dieses Parameters den Pfad zur Schlüsseldatei angeben.	Zeichenfolgenwert.
`webConsoleAccount`	Name des Benutzerkontos, unter dem der Dienst KSCWebConsole ausgeführt wird.	Zeichenkette im folgenden Format: `"Gruppenname:Benutzername"`. Beispiel: `"Gruppe1:Benutzer1"`. Wenn kein Wert angegeben wird, erstellt d von Kaspersky Security Center Web Con Benutzerkonto mit dem Standardnamen u
`managementServiceAccount`	Name des privilegierten Benutzerkontos, unter dem der Dienst KSCWebConsoleManagement ausgeführt wird.	Zeichenkette im folgenden Format: `"Gruppenname:Benutzername"`. Beispiel: `"Gruppe1:Benutzer1"`. Wenn kein Wert angegeben wird, erstellt d von Kaspersky Security Center Web Con Benutzerkonto mit dem Standardnamen u
`serviceWebConsoleAccount`	Name des Benutzerkontos, unter dem der Dienst KSCSvcWebConsole ausgeführt wird.	Zeichenkette im folgenden Format: `"Gruppenname:Benutzername"`. Beispiel: `"Gruppe1:Benutzer1"`. Wenn kein Wert angegeben wird, erstellt d von Kaspersky Security Center Web Con Benutzerkonto mit dem Standardnamen u
`pluginAccount`	Name des Benutzerkontos, unter dem der Dienst KSCWebConsolePlugin ausgeführt wird.	Zeichenkette im folgenden Format: `"Gruppenname:Benutzername"`. Beispiel: `"Gruppe1:Benutzer1"`. Wenn kein Wert angegeben wird, erstellt d von Kaspersky Security Center Web Con Benutzerkonto mit dem Standardnamen u
`messageQueueAccount`	Name des Benutzerkontos, unter dem der Dienst KSCWebConsoleMessageQueue ausgeführt wird.	Zeichenkette im folgenden Format: `"Gruppenname:Benutzername"`. Beispiel: `"Gruppe1:Benutzer1"`. Wenn kein Wert angegeben wird, erstellt d von Kaspersky Security Center Web Con Benutzerkonto mit dem Standardnamen `user_message_queue_%uid%`.

Wenn Sie die Parameter `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` oder `messageQueueAccount` angeben, stellen Sie sicher, dass die benutzerdefinierten Benutzerkonten derselben Sicherheitsgruppe angehören. Wenn diese Parameter nicht angegeben werden, erstellt das Installationsprogramm von Kaspersky Security Center Web Console eine standardmäßige Sicherheitsgruppe und legt anschließend Benutzerkonten mit Standardnamen in dieser Gruppe an.

Kaspersky Security Center Web Console unter Astra Linux in der geschlossenen Softwareumgebung installieren

In diesem Abschnitt wird beschrieben, wie Sie den Server der Kaspersky Security Center Web Console (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. Nennen Sie die Datei "ksc-web-console-setup.json" und platzieren Sie diese in dem folgenden Pfad: /etc/ksc-web-console-setup.json.

   Beispiel für eine Antwortdatei mit minimalem Parametersatz sowie Standardadresse und Standardport:

   ```
   {
     "address": "127.0.0.1",
     "port": "8080",
     "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
     "acceptEula": "true"
   }
   ```

4. Öffnen Sie die Datei `/etc/digsig/digsig_initrafs.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 Programmschlüssel:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

7. Legen Sie den Programmschlüssel `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` in das Verzeichnis ab, das Sie im vorherigen Schritt erstellt haben:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   > Wenn der Programmschlüssel "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 Installationsdatei 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 dpkg -i ksc-web-console-[Build-Nummer].x86_64.deb
```

- Um von einer früheren Version von Kaspersky Security Center Web Console zu aktualisieren, führen Sie den folgenden Befehl aus:
  ```
  $ sudo dpkg -i 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, 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.

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 Kaspersky Security Center Web Console (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.

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 die `vertrauenswürdigen` Installationsparameter an, um dem Kaspersky Security Center Linux Failover-Cluster zu ermöglichen, sich mit der Kaspersky Security Center Web Console zu verbinden. Der Zeichenfolge dieses Parameters hat das folgende Format:
   ```
   "trusted": "Serveradresse|Port|Pfad des Zertifikats|Servername"
   ```
   Geben Sie die Komponenten der `vertrauenswürdigen` Installationsparameter an:

   - **Adresse des Administrationsservers**. Wenn Sie einen sekundären Netzwerkadapter im Rahmen der Vorbereitung der Cluster-Knoten erstellt haben, verwenden Sie die IP-Adresse des Adapters als Adresse für das Kaspersky Security Center Linux Failover-Cluster. Geben Sie andernfalls die IP-Adresse eines von Ihnen verwendeten Load Balancers eines Drittanbieters an.

   - **Port des Administrationsservers**. Der OpenAPI-Port, den Kaspersky Security Center Web Console für die Verbindung mit dem Administrationsserver verwendet (Standardwert ist 13299).

   - **Zertifikat des Administrationsservers**. Das Zertifikat des Administrationsservers befindet sich im freigegebenen Datenspeicher des Kaspersky Security Center Linux Failover-Clusters. Der Standardpfad zur Zertifikatsdatei lautet: <freigegebener Datenordner>\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.

   - **Name des Administrationsservers**. Der Name des Kaspersky Security Center Linux Failover-Clusters, der im Anmeldefenster der Kaspersky Security Center Web Console angezeigt wird.

3. Fahren Sie mit der standardmäßigen Installationsroutine von Kaspersky Security Center Web Console fort.

Nach dem Abschluss der Installation wird auf Ihrem Desktop eine Verknüpfung angezeigt und Sie können sich in der Kaspersky Security Center Web Console anmelden.

Sie können zum Punkt **Gerätesuche und Bereitstellung → Nicht zugeordnete Geräte** wechseln, um Informationen über die Cluster-Knoten und den Dateiserver anzuzeigen.

Kaspersky Security Center Linux Failover-Cluster bereitstellen

Dieser Abschnitt enthält sowohl allgemeine Informationen zum Kaspersky Security Center Linux Failover-Cluster als auch Anweisungen zur Vorbereitung und Bereitstellung des 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.

Erforderliche Vorrausetzungen

Sie verfügen über die Hardware, welche die Anforderungen für das Failover Cluster erfüllt.

Die Bereitstellung von Kaspersky-Programmen erfolgt schrittweise:

1. **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

2. **Vorbereiten von aktiven und passiven Knoten**

   Bereiten Sie zwei Computer mit identischer Hardware und Software vor, um als aktive und passive Knoten zu fungieren.

   Anleitungen: Knoten für Kaspersky Security Center Linux Failover-Cluster vorbereiten

3. **Erstellen von Konten 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 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.

4. **Installieren des Datenbankmanagementsystems (DBMS)**

   Sie haben zwei Optionen:

   - Wenn Sie MariaDB Galera Cluster verwenden möchten, benötigen Sie keinen dedizierten Computer für das DBMS. Installieren Sie MariaDB Galera Cluster auf jedem der Knoten.
   - Wenn Sie ein anderes unterstütztes DBMS verwenden möchten, installieren Sie das ausgewählte DBMS auf einem dedizierten Computer.

5. **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 aktiven Knoten installieren und anschließend auf dem passiven.

   Darüber hinaus können Sie Kaspersky Security Center Web Console auf einem separaten Gerät installieren, das kein Knoten eines Clusters ist.

6. **Testen des Failover-Clusters**

   Überprüfen Sie, ob Sie das Failover Cluster richtig konfiguriert haben und ob es ordnungsgemäß funktioniert. Sie können beispielsweise einen der Dienste von Kaspersky Security Center Linux auf dem aktiven Knoten stoppen: kladminserver, klnagent, ksnproxy, klactprx oder klwebsrv. Wenn der Dienst angehalten wird, muss die Schutzverwaltung automatisch auf den passiven Knoten umschalten.

Ergebnisse

Das Kaspersky Security Center Linux Failover-Cluster wurde bereitgestellt. Bitte informieren Sie sich über die Ereignisse, die zum Umschalten zwischen dem aktiven und passiven Knoten führen.

Über Kaspersky Security Center Linux Failover-Cluster

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.

> 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.

Hard- und Softwarevoraussetzungen

Um ein Kaspersky Security Center Linux Failover-Cluster bereitzustellen, benötigen Sie die folgende Hardware:

- Zwei Computer mit identischer Hard- und Software. Diese Computer fungieren als aktive und passive Knoten.

- Ein Dateiserver unter Linux mit dem EXT4-Dateisystem. Sie müssen einen dedizierten Computer bereitstellen, der als Dateiserver fungiert.

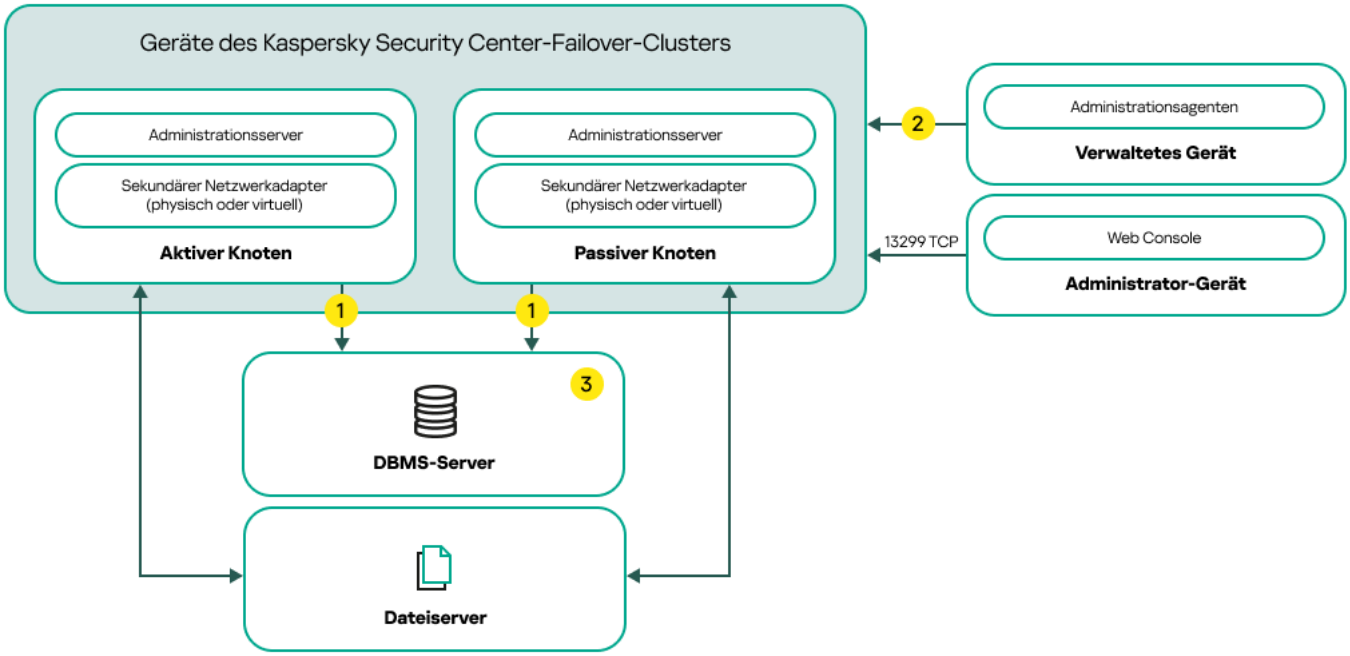
  Stellen Sie sicher, dass Sie eine hohe Netzwerkbandbreite zwischen dem Dateiserver und den aktiven und passiven Knoten bereitgestellt haben.

- Ein Computer mit Datenbankverwaltungssystem (DBMS). Wenn Sie MariaDB Galera Cluster als DBMS verwenden, ist für diesen Zweck kein dedizierter Computer erforderlich.

Bereitstellungsschemata:

Für die Bereitstellung des Kaspersky Security Center Linux-Failover-Cluster können Sie aus den folgenden Schemata auswählen:

- Schema unter Verwendung eines sekundären Netzwerkadapter.
- Schema unter Verwendung eines Drittanbieter-Load-Balancers.



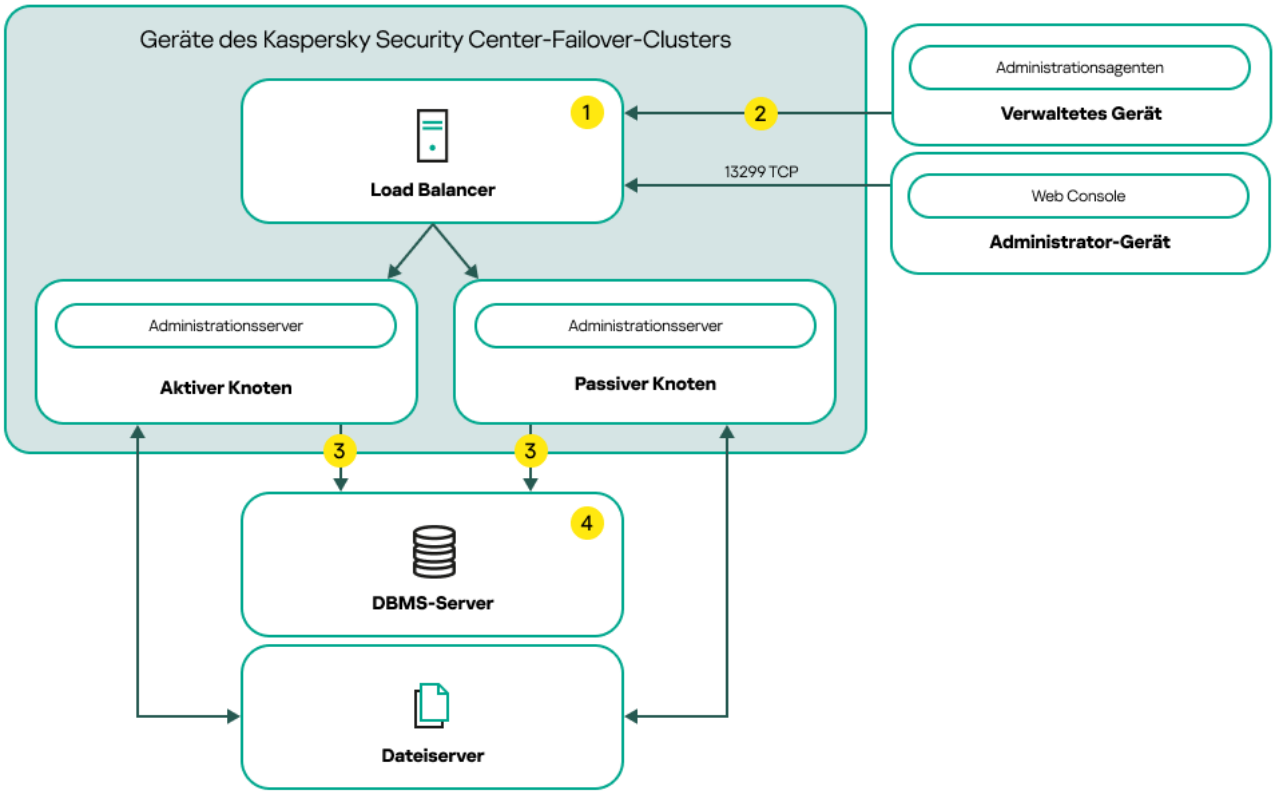
Schema unter Verwendung eines sekundären Netzwerkadapter

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 1433 für Microsoft SQL Server. Relevante Informationen finden Sie in der DBMS-Dokumentation.

2 Öffnen Sie auf den verwalteten Geräten die folgenden Ports: TCP 13000, UDP 13000 und TCP 17000.

3 Computer mit einem Datenbankverwaltungssystem (DBMS). Wenn Sie MariaDB Galera Cluster als DBMS verwenden, ist für diesen Zweck kein dedizierter Computer erforderlich. Installieren Sie MariaDB Galera Cluster auf jedem der Knoten.



Schema unter Verwendung eines Drittanbieter-Load-Balancers

Legende des Schemas:

1 Öffnen Sie auf dem Gerät des Load-Balancers alle Ports des Administrationsservers: TCP 13000, UDP 13000, TCP 13291, TCP 13299 und TCP 17000.

2 Öffnen Sie auf den verwalteten Geräten die folgenden Ports: 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 1433 für Microsoft SQL Server. Relevante Informationen finden Sie in der DBMS-Dokumentation.

4 Computer mit einem Datenbankverwaltungssystem (DBMS). Wenn Sie MariaDB Galera Cluster als DBMS verwenden, ist für diesen Zweck kein dedizierter Computer erforderlich. Installieren Sie MariaDB Galera Cluster auf jedem der Knoten.

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 vom Benutzer absichtlich beendet. Die Dienste von Kaspersky Security Center Linux sind: kladminserver, klnagent, klactprx und klwebsrv.
- Die Netzwerkverbindung zwischen dem aktiven Knoten und dem Speicher auf dem Dateiserver wurde unterbrochen oder beendet.

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
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.

   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
   ```

   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 777 /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,exec,sync,no_subtree_check,no_root_squash\) >> /etc/exports"
   sudo exportfs -a
   sudo systemctl start rpcbind
   sudo service nfs start
   ```

   Aktivieren Sie den Autostart, indem Sie den folgenden Befehl ausführen:

   ```
   sudo systemctl enable rpcbind
   ```

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

Bereiten Sie zwei Computer darauf vor, als aktiver und passiver Knoten für das Kaspersky Security Center Linux Failover-Cluster zu fungieren.

Um die Knoten für das Kaspersky Security Center Linux Failover-Cluster vorzubereiten:

1. Stellen Sie sicher, dass Sie über zwei Computer verfügen, welche die Hardware- und Softwareanforderungen erfüllen. Diese Computer fungieren als aktive und passive Knoten des Failover-Clusters.

2. 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:
   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

3. Erstellen Sie Einhängepunkte, indem Sie die folgenden Befehle ausführen:
   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```
   ,

4. Passen Sie die Einhängepunkte und die freigegebenen Ordner an:
   ```
   sudo sh -c "echo {server}:{path to the KlFocStateShare folder} /mnt/KlFocStateShare
   nfs vers=4,nolock,local_lock=none,auto,user,rw 0 0 >> /etc/fstab"
   sudo sh -c "echo {server}:{path to the KlFocDataShare_klfoc folder}
   /mnt/KlFocDataShare_klfoc nfs vers=4,nolock,local_lock=none,noauto,user,rw 0 0 >>
   /etc/fstab
   ```
   Dabei sind `{server}:{path to the KlFocStateShare folder}` und `{server}:{path to the KlFocDataShare_klfoc folder}` die Netzwerkpfade der freigegebenen Ordner auf dem Dateiserver.

5. Stellen Sie die freigegebenen Ordner bereit, indem Sie die folgenden Befehle ausführen:
   ```
   mount /mnt/KlFocStateShare
   mount /mnt/KlFocDataShare_klfoc
   ```

6. Stellen Sie sicher, dass die Berechtigungen für den Zugriff auf die freigegebenen Ordner ksc:kladmins gehören.

   Führen Sie den folgenden Befehl aus:
   ```
   sudo ls -la /mnt/
   ```

7. Konfigurieren Sie auf jedem der Knoten einen sekundären Netzwerkadapter.

   Ein sekundärer Netzwerkadapter kann physisch oder virtuell sein. Wenn Sie einen physischen Netzwerkadapter verwenden möchten, schließen Sie ihn an und konfigurieren Sie ihn mit den Standardtools des Betriebssystems. Wenn Sie einen virtuellen Netzwerkadapter verwenden möchten, erstellen Sie ihn mithilfe von Drittanbieter-Software.

   Führen Sie eine der folgenden Aktionen aus:

   - Verwenden Sie einen virtuellen Netzwerkadapter.

     a. Verwenden Sie den folgenden Befehl, um zu überprüfen, ob zum Verwalten des physischen Adapters der NetworkManager verwendet wird:
        ```
        nmcli device status
        ```

        Wenn der physische Adapter in der Ausgabe als nicht verwaltet angezeigt wird, konfigurieren Sie den NetworkManager für die Verwaltung des physischen Adapters. Die genauen Konfigurationsschritte hängen von Ihrer Distribution ab.

b. Verwenden Sie den folgenden Befehl, um Schnittstellen zu identifizieren:

```
ip a
```

c. Erstellen Sie ein neues Konfigurationsprofil:

```
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 Netzwerkadapter oder einen Hypervisor. Deaktivieren Sie in diesem Szenario das Programm NetworkManager.

  a. Löschen Sie die NetworkManager-Verbindungen für die Zielschnittstelle:

  ```
  nmcli con del <Verbindungsname>
  ```

  Verwenden Sie den folgenden Befehl, um zu überprüfen, ob die Zielschnittstelle noch Verbindungen besitzt:

  ```
  nmcli con show
  ```

  b. Bearbeiten Sie die Datei "NetworkManager.conf". Suchen Sie den Abschnitt "keyfile" und weisen Sie die Zielschnittstelle dem Parameter "unmanaged-devices" zu.

  ```
  [keyfile]
  unmanaged-devices=interface-name:<Schnittstellenname>
  ```

  c. Starten Sie den NetworkManager neu:

  ```
  systemctl reload NetworkManager
  ```

  Verwenden Sie den folgenden Befehl, um zu überprüfen, dass die Zielschnittstelle nicht verwaltet wird:

  ```
  nmcli dev status
  ```

- Verwenden Sie den Load Balancer eines Drittanbieters. Sie können beispielsweise einen nginx-Server verwenden. Gehen Sie in diesem Fall wie folgt vor:

  a. Stellen Sie einen dedizierten Linux-basierten Computer mit installiertem nginx bereit.

  b. Konfigurieren Sie das Load Balancing. Legen Sie den aktiven Knoten als Hauptserver und den passiven Knoten als Backup-Server fest.

  c. Öffnen Sie auf dem nginx-Server alle Ports des Administrationsservers: TCP 13000, UDP 13000, TCP 13291, TCP 13299, TCP 17000.

Die Knoten sind vorbereitet. Um das Kaspersky Security Center Linux Failover-Cluster bereitzustellen, folgen Sie den weiteren Anweisungen des Szenarios.

Kaspersky Security Center Linux auf den Knoten des Kaspersky Security Center Linux Failover-Clusters installieren

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 das Programm 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.

Verwenden Sie die Installationsdatei ksc64_[Versionsnummer]_amd64.deb oder ksc64-[Versionsnummer].x86_64.rpm, die der auf Ihrem Gerät installierten Linux-Distribution entspricht. Sie erhalten die Installationsdatei, indem Sie diese von der Kaspersky-Website herunterladen.

Installation auf dem primären (aktiven) Knoten

Um Kaspersky Security Center Linux auf dem primären 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 in der Befehlszeile die Befehle aus dieser Anleitung aus.

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 install /<path>/ksc64_[Versionsnummer]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[Versionsnummer].x86_64.rpm -y`

4. Führen Sie die Konfiguration von Kaspersky Security Center Linux aus:

   ```
   sudo /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 ein:

   a. Geben Sie den lokalen Pfad zum State Share-Einhängepunkt ein.

   b. Geben Sie den lokalen Pfad zum Data Share-Einhängepunkt ein.

   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. Wenn Sie aufgefordert werden, den DNS-Namen oder die statische IP-Adresse des Administrationsservers einzugeben, geben Sie die IP-Adresse des sekundären Netzwerkadapters oder die IP-Adresse des externen Load Balancers ein.

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 vernetzte Geräte den Wert 1 ein.
- Geben Sie für 101 bis 1.000 vernetzte Geräte den Wert 2 ein.
- Geben Sie für über 1.000 vernetzte Geräte den Wert 3 ein.

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 des Datenbank-Root-Benutzerkontos ein, das Sie für den Zugriff auf die Datenbank verwenden.

p. Geben Sie das Kennwort des Datenbank-Root-Benutzerkontos ein, das Sie für den Zugriff auf die Datenbank verwenden.

8. Warten Sie, bis die Dienste hinzugefügt und automatisch gestartet wurden:

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

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.

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 in der Befehlszeile die Befehle aus dieser Anleitung aus.
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 install /<path>/ksc64_[Versionsnummer]_amd64.deb`
   - `sudo yum install /<path>/ksc64-[Versionsnummer].x86_64.rpm -y`
4. Führen Sie die Konfiguration von Kaspersky Security Center Linux aus:
   `sudo /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 **Sekundärer Cluster-Knoten** als Installationsmodus des Administrationsservers aus.
7. Geben Sie bei Aufforderung den lokalen Pfad des State Share-Einhängepunkts ein.

Kaspersky Security Center Linux wird auf dem sekundären Knoten installiert.

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`

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:

1. Gehen Sie im aktiven Knoten zu /opt/kaspersky/ksc64/sbin.
2. Öffnen Sie die Befehlszeile und führen Sie einen der folgenden Befehle aus:
   - Um das Cluster zu stoppen: `klfoc -stopcluster --stp klfoc`
   - Um das Cluster zu starten: `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`.

Der Knoten ist gewartet und an das Failover-Cluster angehängt.

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 Datenbank des Administrationsservers:
  - **Automatisch**. Während der Installation des Administrationsservers können Sie automatisch eine Datenbank für den Administrationsserver anlegen (auch als Serverdatenbank bezeichnet) indem Sie das Installationsprogramm des Administrationsservers (den Installer) verwenden.
  - **Manuell**. Sie können eine Anwendung eines Drittanbieters 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.

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:
  - Datenbank des Administrationsservers: 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.

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 Datenbank des Administrationsservers: ALL. • Privilegien für alle Tabellen im Schema "public": ALL. • Privilegien für alle Sequenzen im Schema "public": ALL.

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 Datenbank des Administrationsservers 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.

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:

   ```
   /* Erstellen eines Benutzers namens KSCAdmin und angeben des Kennworts für KSCAdmin */
   CREATE USER 'KSCAdmin' IDENTIFIED BY '<Kennwort>';
   ```

   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 'KSCAdmin'@'%' 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 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<Kennwort>';
     ```

3. Gewähren Sie dem erstellten DBMS-Konto die folgenden Privilegien:

   - Schema-Privilegien:
     - Datenbank des Administrationsservers: 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:

   ```
   /* KSCAdmin Berechtigungen gewähren */
   GRANT USAGE ON *.* TO 'KSCAdmin';
   GRANT ALL ON kav.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
   GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
   GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
   GRANT PROCESS ON *.* TO 'KSCAdmin';
   GRANT SUPER ON *.* TO 'KSCAdmin';
   ```

   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 'KSCAdmin'`.

4. Führen Sie den folgenden Befehl aus, um die Liste der Berechtigungen anzuzeigen, die dem DBMS-Konto gewährt wurden:

   ```
   SHOW grants for 'KSCAdmin';
   ```

5. Um eine Datenbank des Administrationsservers manuell zu erstellen, führen Sie das folgende Skript aus (in diesem Skript lautet der Name der Datenbank des Administrationsservers *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET utf8
   DEFAULT COLLATE utf8_general_ci;
   ```

   Verwenden Sie denselben Datenbanknamen, den Sie in dem Skript angeben, welches das DBMS-Konto erstellt.

6. Installieren Sie den Administrationsserver.

Nach Abschluss der Installation wird die Datenbank des Administrationsservers 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.

Konfigurieren des DBMS-Kontos für die Installation des Administrationsservers (automatisches Erstellen der Datenbank des Administrationsservers)

So konfigurieren Sie das DBMS-Benutzerkonto für die Installation des Administrationsservers:

1. Starten Sie eine Umgebung für die Arbeit mit PostgreSQL und Postgres Pro.
2. Wählen Sie eine Postgres-Rolle aus, um auf das DBMS zuzugreifen. Sie können eine der folgenden Rollen verwenden:

   - Den Benutzer *Postgres* (standardmäßige Postgres-Rolle).

     Wenn Sie den Benutzer *Postgres* verwenden, müssen Sie ihm keine zusätzlichen Rechte gewähren.

     Standardmäßig besitzt der Benutzer *Postgres* kein Kennwort. Ein Kennwort ist jedoch für die Installation von Kaspersky Security Center Linux erforderlich. Um für den Benutzer *Postgres* ein Kennwort einzurichten, führen Sie das folgende Skript aus:

     ```
     ALTER USER "user_name" WITH PASSWORD '<Kennwort>';
     ```

   - Eine neue Postgres-Rolle.

     Wenn Sie eine neue Postgres-Rolle verwenden möchten, erstellen Sie diese Rolle und erteilen Sie ihr anschließend das Privileg CREATEDB. Führen Sie dazu folgendes Skript aus (in diesem Skript lautet die Rolle *KCSAdmin*):

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<Kennwort>' CREATEDB;
     ```

     Die erstellte Rolle wird als Besitzer der Datenbank des Administrationsservers (im Folgenden auch als Serverdatenbank bezeichnet) verwendet.

3. Installieren Sie den Administrationsserver.

Nach Abschluss der Installation wird die Serverdatenbank automatisch erstellt und der Administrationsserver ist einsatzbereit.

Konfigurieren des DBMS-Kontos für die Installation des Administrationsservers (manuelles Erstellen der Datenbank des Administrationsservers)

So konfigurieren Sie das DBMS-Benutzerkonto für die Installation des Administrationsservers:

1. Starten Sie eine Umgebung für die Arbeit mit Postgres.

2. Erstellen Sie eine neue Postgres-Rolle und eine Datenbank für den Administrationsserver. Erteilen Sie der Rolle in der Datenbank des Administrationsservers anschließend alle Berechtigungen. Melden Sie sich dazu als Benutzer *Postgres* an der Datenbank *Postgres* an und führen Sie anschließend das folgende Skript aus (in diesem Skript lautet die Rolle *KCSAdmin* und der Name der Datenbank des Administrationsservers *KAV*):

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '<Kennwort>';
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   > 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 "KSCAdmin" TEMPLATE template0;`
   > anstelle des Befehls:
   > `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

3. Gewähren Sie der erstellten Postgres-Rolle die folgenden Privilegien:

   - Privilegien für alle Tabellen im Schema "public": ALL
   - Berechtigungen für alle Sequenzen im Schema "public": ALL

   Melden Sie sich dazu als Benutzer *Postgres* an der Serverdatenbank an und führen Sie anschließend das folgende Skript aus (in diesem Skript lautet die Rolle *KCSAdmin*):

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

4. Installieren Sie den Administrationsserver.

Nach Abschluss der Installation verwendet der Administrationsserver die erstellte Datenbank zum Speichern der Daten des Administrationsservers. Der Administrationsserver ist einsatzbereit.

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 des Programms zu ermöglichen, verwendet Kaspersky Security Center die folgenden Arten von Zertifikaten:

- Zertifikat des Administrationsservers
- Zertifikat des Webservers
- Zertifikat der Kaspersky Security Center Web Console

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. 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

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 beim Verbinden mit Kaspersky Security Center Web Console
- 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.

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.

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.

Zertifikat des Webservers

Die Webserver-Komponente des Kaspersky Security Center Administrationsservers verwendet eine spezielle Art von Zertifikat. Dieses Zertifikat ist für die Veröffentlichung von Administrationsagenten-Installationspaketen erforderlich, die Sie anschließend auf verwaltete Geräte herunterladen. Aus diesem Grund kann der Webserver verschiedene Zertifikate verwenden.

Der Webserver verwendet eines der folgenden Zertifikate in der Reihenfolge ihrer Priorität:

1. Benutzerdefiniertes Zertifikat des Webservers, das Sie manuell in der Kaspersky Security Center Web Console angegeben haben

2. Gewöhnliches Zertifikate des Administrationsservers ("C")

Zertifikat der Kaspersky Security Center Web Console

Der Server der Kaspersky Security Center Web Console (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.

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: • CA: true • Path Length Constraint: None Schlüsselverwendung: • Digital signature • Certificate signing • Key encipherment • CRL Signing Extended Key Usage (optional): Serverauthentifizierung, Clientauthentifizierung	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	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. 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

Die meisten Browser legen dem Zeitraum für die Gültigkeit eines Zertifikats ein Obergrenze auf. Um innerhalb dieser Begrenzung zu bleiben ist der Gültigkeitszeitraum des Zertifikats von Kaspersky Security Center Web Console auf 397 Tage begrenzt. Sie können ein existierendes Zertifikat ersetzen, das von einer Zertifizierungsstelle (Certification Authority, CA) stammt. Dazu stellen Sie ein neues selbstsigniertes Zertifikat aus. Als Alternative können Sie Ihr abgelaufenes Zertifikat von Kaspersky Security Center Web Console erneut ausstellen.

Des 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 Sie der Browser möglicherweise darüber, dass die Verbindung zu Kaspersky Security Center Web Console nicht privat 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 der Kaspersky Security Center Web Console nach der Neuausstellung der Liste mit vertrauenswürdigen Browser-Zertifikaten hinzu. Es wird empfohlen, dass Sie diese Option nur verwenden, wenn Sie kein benutzerdefiniertes Zertifikat erstellen können.

Um ein abgelaufenes Zertifikat von Kaspersky Security Center Web Console erneut auszustellen:

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 eine Installationsdatei einer aktualisierten Version verwenden möchten, führen Sie den Upgrade-Befehl aus.

Das Zertifikat von Kaspersky Security Center Web Console wurde erneut für einen weiteren Gültigkeitszeitraum von 397 Tagen ausgestellt.

Zertifikat für Kaspersky Security Center Web Console ersetzen

Wenn Sie den Server der Kaspersky Security Center Web Console (auch Kaspersky Security Center Web Console genannt) installieren, wird standardmäßig automatisch ein Browser-Zertifikat für das Programm 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. Erstellen Sie eine neue Antwortdatei, die für die Installation von Kaspersky Security Center Web Console erforderlich ist.

2. Geben Sie in dieser Datei die Pfade der benutzerdefinierten Zertifikatsdatei und der Schlüsseldatei an. Verwenden Sie dazu den Parameter `certPath` und den Parameter `keyPath`.

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' > Schlüssel.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 Schlüssel.pem -out Schlüssel-ohne-Kennwort.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

Das neue Zertifikat muss im PKCS#12-Format erstellt werden (z. B. mittels PKI der Organisation) und von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt werden. Außerdem muss das neue Zertifikat die gesamte Vertrauenskette und einen privaten Schlüssel enthalten, welcher in der Datei mit der pfx- oder p12-Erweiterung gespeichert werden muss. Für das neue Zertifikat müssen unten aufgeführten Voraussetzungen erfüllt sein.

Zertifikatstyp: Gewöhnliches Zertifikat, gewöhnliches Reservezertifikat ("C", "CR")

Voraussetzungen:

- Minimale Schlüssellänge: 2048
- Basic constraints:
  - CA: true
  - Path Length Constraint: None

    Der Wert von "Path Length Constraint" (Einschränkung der Pfadlänge) kann eine von "None" abweichende ganze Zahl sein, darf aber nicht kleiner als 1 sein.
- Schlüsselverwendung:
  - Digital signature
  - Certificate signing
  - Key encipherment
  - 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.

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.

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 Dienstprogramm klsetsrvcert ersetzen

So ersetzen Sie das Zertifikat des Administrationsservers:

Führen Sie aus der Befehlszeile das folgenden Dienstprogramm aus:

```
klsetsrvcert [-t <Typ> {-i <Eingabedatei> [-p <Kennwort>] [-o <chkopt>] | -g <DNS-Name>}][-f <Zeit>][-r <calistfile>][-l <Protokolldatei>]
```

Sie müssen das Dienstprogramm klsetsrvcert nicht herunterladen. Dieses Tool gehört zum Programmpaket von Kaspersky Security Center Linux. Es ist nicht mit früheren Versionen von Kaspersky Security Center Linux kompatibel.

Die Beschreibung der Parameter des Dienstprogramms klsetsrvcert finden Sie in der folgenden Tabelle.

Parameterwerte des Dienstprogramms klsetsrvcert

Parameter	Wert
`-t <Typ>`	Typ des Zertifikats, das ersetzt werden muss. Mögliche Einstellungswerte des Parameters `<Typ>`: • `C` – gewöhnliches Zertifikat für die Ports 13000 und 13291 ersetzen. • `CR` – gewöhnliches Reservezertifikat für die Ports 13000 und 13291 ersetzen.
`-f <Zeit>`	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 gewöhnliche Zertifikat oder das gewöhnliche Reservezertifikat ersetzen möchten, bevor es abläuft. Geben Sie die Zeit an, zu der verwaltete Geräte mit dem Administrationsserver mit einem neuen Zertifikat synchronisiert werden müssen.
`-I <Eingabedatei>`	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.
`-o <chkopt>`	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>`	Ein neues Zertifikat wird für den angegebenen DNS-Namen erstellt.
`-r <calistfile>`	Liste mit vertrauenswürdigen Zertifizierungsstellen für Stammzertifikate im Format PEM.
`-l <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 <Eingabedatei> -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 <Eingabedatei> -p <Kennwort> -o NoCA
```

2. Um ein Datum anzugeben, an dem das Zertifikat angewendet wird:

```
klsetsrvcert -f "DD-MM-YYYY hh:mm"
```

Wobei `TT-MM-JJJJ hh:mm` das Datum 3-4 Wochen nach dem aktuellen Datum darstellt. Der zeitliche Versatz ist zum Auswechseln des Zertifikats durch ein neues vorgesehen und ermöglicht die Verteilung dieses neuen Zertifikats an alle Administrationsagenten.

Administrationsagenten mit dem Administrationsserver mittels Dienstprogramm klmover verbinden

Nachdem Sie das Zertifikat des Administrationsservers mit dem Dienstprogramm klsetsrvcert über die Befehlszeile ersetzt haben, müssen Sie die SSL-Verbindung zwischen den Administrationsagenten und dem Administrationsserver herstellen, da die Verbindung unterbrochen wurde.

So geben Sie das neue Zertifikat des Administrationsservers an und stellen die Verbindung wieder her:

Führen Sie aus der Befehlszeile das folgenden Dienstprogramm aus:

```
klmover [-address <Serveradresse>] [-pn <Portnummer>] [-ps <SSL-Portnummer>] [-nossl]
[-cert <Pfad zur Zertifikatsdatei>]
```

Das Dienstprogramm wird automatisch in den Installationsordner des Administrationsagenten kopiert, wenn der Administrationsagent auf einem Client-Gerät installiert wird.

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. Für Geräte, die ohne lokale Administratorrechte betrieben werden, kann der Kennwortschutz für die Ausführung des Tools "klmover" ausgelassen werden.

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

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.

Neuausstellung des Webserver-Zertifikats

Das in Kaspersky Security Center Linux verwendete Zertifikat des Webservers wird für die Veröffentlichung von Installationspaketen des Administrationsagenten, die Sie anschließend auf Ihre verwalteten Geräte herunterladen, genauso benötigt, wie 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 unter Zertifikate von Kaspersky Security Center Linux).

Wenn Sie im Abschnitt **Webserver** des Eigenschaftenfensters des Administrationsservers noch nie ein eigenes benutzerdefiniertes Zertifikat als Webserver-Zertifikat angegeben haben, fungiert 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 erneut aus, wenn Sie keine mobilen 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. Überprüfen Sie, ob Ihr benutzerdefiniertes Zertifikat den Anforderungen von Kaspersky Security Center Linux und den Anforderungen an vertrauenswürdige Zertifikate von Apple entspricht. Ändern Sie gegebenenfalls das Zertifikat.

   Sie können das Hilfsprogramm kliossrvcertgen.exe verwenden, um ein Zertifikat zu generieren.

2. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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 **Anderes Zertifikat angeben** aus und klicken Sie auf die Schaltfläche **Zertifikat ändern**.

5. Wählen Sie im folgenden Fenster im Feld **Zertifikatstyp** den Typ Ihres Zertifikats aus:

   - Wenn Sie **Container PKCS#12** ausgewählt haben, klicken Sie auf die Schaltfläche **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 (falls vorhanden)** ein.

   - Wenn Sie **X.509-Zertifikat** ausgewählt haben, klicken Sie auf die Schaltfläche **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 (falls vorhanden)** ein.

6. Klicken Sie auf die Schaltfläche **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 die Schaltfläche **Speichern**.

Das Webserver-Zertifikat wird erneut ausgestellt.

So stellen Sie das Webserver-Zertifikat erneut aus, wenn Sie keine mobilen Geräte über das mobile Protokoll verwaltet haben:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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 die Schaltfläche **Durchsuchen**.

   b. Wählen Sie im folgenden Fenster in der Gruppe für die Einstellungen **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. Überprüfen Sie, ob Ihr benutzerdefiniertes Zertifikat den Anforderungen von Kaspersky Security Center Linux und den Anforderungen an vertrauenswürdige Zertifikate von Apple entspricht. Ändern Sie gegebenenfalls das Zertifikat.

b. Wählen Sie die Option **Anderes Zertifikat** aus, klicken Sie auf die Schaltfläche **Zertifikat verwalten** und klicken Sie anschließend im angezeigten Fenster auf die Schaltfläche **Durchsuchen**.

c. Wählen Sie im folgenden Fenster im Feld **Zertifikatstyp** den Typ Ihres Zertifikats aus:

- Wenn Sie **Container PKCS#12** ausgewählt haben, klicken Sie auf die Schaltfläche **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 (falls vorhanden)** ein.
- Wenn Sie **X.509-Zertifikat** ausgewählt haben, klicken Sie auf die Schaltfläche **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 (falls vorhanden)** ein.

d. Klicken Sie auf die Schaltfläche **Speichern** und anschließend auf **OK**.

Das Mobilgerät-Zertifikat wird erneut ausgestellt, um als Webserver-Zertifikat verwendet zu werden.

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.

Um sich in der Kaspersky Security Center Web Console anzumelden, gehen Sie wie folgt vor:

1. Rufen Sie in Ihrem Browser <Webadresse des Administrationsservers>:<Port> auf.

   Die Anmeldeseite 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 Administrationsserver hinzugefügt haben, ist die Liste mit Administrationsservern gesperrt.

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 **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**.

Nach der Anmeldung wird das Dashboard in der Sprache und dem Design angezeigt, das 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 Hauptmenü zu Ihren Kontoeinstellungen 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 Teil des Fensters
- Arbeitsbereich im rechten Teil des Fensters

Hauptmenü

Das Hauptmenü enthält die folgenden Abschnitte:

- **Administrationsserver**. Zeigt den Namen des Administrationsservers an, mit dem Sie aktuell verbunden sind. Klicken Sie auf das Einstellungssymbol (), um die Eigenschaften des Administrationsservers zu öffnen.
- **Überwachung und Berichterstattung**. Bietet Ihnen einen Überblick über Ihre Infrastruktur, den Schutzstatus und die Statistiken.
- **Assets (Geräte)**. Enthält Werkzeuge für Assets, Aufgaben und Richtlinien der Kaspersky-Anwendungen.
- **Benutzer und Rollen**. Erlaubt Ihnen Benutzer und Rollen zu verwalten, Benutzerrechte durch das Zuweisen von Rollen an Benutzer zu konfigurieren und Richtlinienprofile mit Rollen zu verknüpfen.
- **VORGÄNGE**. Enthält eine Vielzahl von Vorgängen wie die Anwendungslizenzierung, das Anzeigen und Verwalten von verschlüsselten Laufwerken sowie Verschlüsselungsereignissen und die Verwaltung von Drittanbieter-Anwendungen. Dies umfasst auch den Zugriff auf die Datenverwaltungen der Anwendung.
- **Entdeckung und Bereitstellung**. Ermöglicht Ihnen das Durchführen von Netzwerkabfragen zum Auffinden von Client-Geräten sowie die manuelle oder automatische Verteilung dieser Geräte an Administrationsgruppen. Dieser Abschnitt umfasst außerdem den Schnellstartassistenten und den Assistenten für die Bereitstellung des Schutzes.
- **Marketplace**. Enthält Informationen über den kompletten Umfang an Business-Lösungen von Kaspersky und ermöglicht es Ihnen, die erforderlichen Lösungen auszuwählen und anschließend auf der Kaspersky-Website zu erwerben.

- **Einstellungen**. Erlaubt Ihnen, den aktuellen Zustand eines Web-Plug-ins zu sichern, um den gespeicherten Zustand später wiederherstellen zu können. Enthält Ihre persönlichen Einstellungen für die Darstellung der Benutzeroberfläche, z. B. die gewählte Sprache für die Benutzeroberfläche oder das Farbschema.

- **Menü Ihres Benutzerkontos**. Enthält einen Link zur Hilfe von Kaspersky Security Center Linux. Sie sich außerdem von Kaspersky Security Center Linux abmelden und die Version von Kaspersky Security Center Web Console sowie die Liste der installierten Verwaltungs-Plug-ins 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 konfigurieren können.

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. Wechseln Sie im Hauptmenü zu **Einstellungen** → **Sprache**.

2. Wählen Sie eine der unterstützten Lokalisierungssprachen aus.

Abschnitte des Hauptmenüs anheften und lösen

Sie können Abschnitte von Kaspersky Security Center Web Console anheften, um sie Ihren Favoriten hinzuzufügen und sie schnell über den Abschnitt **Angepinnt** des Hauptmenüs zu erreichen.

> Wenn keine angehefteten Elemente vorhanden sind, wird der Abschnitt **Angepinnt** nicht im Hauptmenü angezeigt.

Sie können nur Abschnitte anheften, in denen Seiten angezeigt werden. Wenn Sie beispielsweise zum Abschnitt **Assets (Geräte)** → **Verwaltete Geräte** wechseln, wird die Seite mit der Gerätetabelle geöffnet. Dies bedeutet, dass Sie den Abschnitt **Verwaltete Geräte** anheften können. Sollte hingegen ein Fenster oder kein Element angezeigt werden, nachdem Sie einen Abschnitt im Hauptmenü ausgewählt haben, können Sie den ausgewählten Abschnitt nicht anheften.

So können Sie einen Abschnitt anheften:

1. Bewegen Sie den Mauszeiger im Hauptmenü über den Abschnitt, den Sie anheften möchten.

   Das Pin-Symbol (📌) wird angezeigt.

2. Klicken Sie auf das Pin-Symbol (📌).

Der Abschnitt wird angeheftet und im Abschnitt **Angepinnt** angezeigt.

Sie können bis zu fünf Elemente anheften.

Sie können auch Elemente aus Ihren Favoriten entfernen, indem Sie diese lösen.

So lösen Sie einen angehefteten Abschnitt:

1. Wechseln Sie im Hauptmenü zum Abschnitt **Angepinnt**.
2. Bewegen Sie den Mauszeiger über den Abschnitt, den Sie lösen möchten, und klicken Sie anschließend auf das Lösen-Symbol ( ).

Der Abschnitt wird aus Ihren Favoriten entfernt.

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 am Programm 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 Arbeitsstationen und Server sowie Aufgaben zur Schadsoftware-Untersuchung, Update-Download und Verschieben ins Backup für die oberste Hierarchieebene der verwalteten Geräte erstellen.

  Der Schnellstartassistent erstellt Richtlinien nur für die Programme, deren Ordner **Verwaltete 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.

Das Programm 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 das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Allgemein** aus.
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-Programme 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:

- **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.

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 Programmverwaltungs-Plug-ins und für die Programmpakete auf den Kaspersky-Servern an, die Sie herunterladen und auf Client-Geräten in Ihrem Netzwerk installieren können. Wählen Sie die Optionen aus:

- **Bereiche**

  Sie können die folgenden Schutzbereiche auswählen:

  - **Workstations**
  - **Dateiserver und Datenspeicherungssysteme**
  - **Virtualisierung**
  - **Embedded Systeme**
  - **Industrielle Netzwerke**
  - **Industrielle Endpunkte**

- **Betriebssysteme**

  Sie können folgende Plattformen wählen:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Anderes

  Informationen zu unterstützten Betriebssystemen finden Sie im Abschnitt "Hardware- und Softwarevoraussetzungen für die Kaspersky Security Center Web Console".

Das Auswählen der Kaspersky-Programmpakete aus der Liste der verfügbaren Pakete kann später unabhängig vom Schnellstartassistenten durchgeführt werden. 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.

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 Programme. 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. Die Liste der Plug-ins umfasst die folgenden Spalten:

- **Zu schützender Bereich**

  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-Programme 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 für 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 Programme 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.

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-Programme 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. Wählen Sie eine der folgenden Varianten aus:

- **Ich akzeptiere die Nutzungsbedingungen für Kaspersky Security Network**

  Kaspersky Security Center Linux und die verwalteten Programme, 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 für Kaspersky Security Network ab**

  Kaspersky Security Center Linux und verwaltete Programme 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 das Programm 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 für Kaspersky-Software** 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 des Programms hinzuzufügen.

Sie erhalten Ihre Schlüsseldatei an die E-Mail-Adresse, die Sie beim Kauf von Kaspersky Security Center angegeben haben.

Um das Programm 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 für Kaspersky-Software** des Hauptmenüs an die verwalteten Geräte bereitstellen.

- Verschieben Sie die Aktivierung des Programms

Wenn Sie die verschobene Aktivierung des Programms 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. Festlegen der Einstellungen zur Verwaltung von Drittanbieter-Updates

Im Schnellstartassistenten wird der Schritt **Einstellungen für die Verwaltung von Updates** wird 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.

Wählen Sie für Software-Updates von Drittanbietern eine der folgenden Varianten aus:

- **Nach benötigten Updates suchen**

  Falls die die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* noch nicht vorhanden ist, wird automatisch erstellt.

  Diese Variante ist standardmäßig festgelegt.

- **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 Variante ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Wählen Sie für die Updates von Windows-Update die Option **Die in der Domänenrichtlinie angegeben Update-Quellen verwenden** aus.

Die Client-Geräte laden Windows-Updates in Übereinstimmung mit 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.

Schritt 11. E-Mail-Benachrichtigungen konfigurieren

Passen Sie die Einstellungen für den Versand von Benachrichtigungen über Ereignisse an, die bei der Ausführung von Kaspersky-Programmen auf den Client-Geräten registriert werden. Diese Einstellungen werden in den Richtlinien für die Anwendungen als Standardwerte verwendet.

Folgende Einstellungen für den Versand von Benachrichtigungen über auftretende Ereignisse der Programme von Kaspersky können angepasst werden:

- **Empfänger (E-Mail-Adressen)**

  E-Mail-Adressen des Nutzers, an die das Programm Benachrichtigungen versenden soll. Sie können eine oder mehrere Adressen angeben. Geben Sie mehrere Adressen durch Semikolon getrennt an.

- **SMTP-Serveradresse**

  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.

Nachdem Sie den Schnellstartassistenten abgeschlossen haben, können Sie den Assistenten für die Bereitstellung des Schutzes ausführen um Anti-Virus-Programme oder den Administrationsagenten automatisch auf Geräten in Ihrem Netzwerk zu installieren.

Assistent für die Bereitstellung des Schutzes

Um Programme von Kaspersky zu installieren, können Sie den Assistenten für die Bereitstellung des Schutzes verwenden. Der Assistent für die Bereitstellung des Schutzes ermöglicht die Remote-Installation von Programmen 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 **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → 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 eines Programms**.

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.

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:

Wechseln 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 1. Installationspaket auswählen

Wählen Sie das Installationspaket des Programms, das Sie installieren möchten.

Wenn das Installationspaket des gewünschten Programms nicht aufgeführt ist, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie dann das Programm aus der Liste aus.

Schritt 2. 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.

Schritt 3. Auswählen der Version des Administrationsagenten

Wenn Sie das Installationspaket eines anderen Programms ausgewählt haben (nicht den Administrationsagenten), müssen Sie auch den Administrationsagenten installieren, da dieser das Programm mit dem Kaspersky Security Center Administrationsserver verbindet.

Wählen Sie die aktuellste Version des Administrationsagenten aus.

Schritt 4. Geräte auswählen

Geben Sie eine Liste mit Geräte an, auf denen das Programm 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 festlegen.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

Schritt 5. Einstellungen für die Aufgabe zur Remote-Installation festlegen

Passen Sie auf der Seite **Einstellungen für die Aufgabe zur Remote-Installation** die Einstellungen für die Remote-Installation eines Programms.

Wählen Sie in der Einstellungsgruppe **Download des Installationspakets erzwingen** die Methode der Übertragung der zur Programminstallation 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, ein Windows-Programm (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 also ein Windows-Programm 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:

- **Programm nicht neu installieren, wenn es bereits installiert ist**

  Wenn diese Option aktiviert ist, wird das ausgewählte Programm nicht neu installiert, wenn es bereits auf dem Client-Gerät installiert ist.

  Wenn Sie dieses Kontrollkästchen deaktivieren, wird das Programm 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.

Schritt 6. 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. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) 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 Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

- **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. 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. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

    Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

  - **Neu starten 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 das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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.

Schritt 7. Deinstallieren inkompatibler Programme vor der Installation

Dieser Schritt ist nur dann verfügbar, wenn das zu verteilende Programm bekanntlich mit anderen Programmen inkompatibel ist.

Wählen Sie diese Option, wenn Sie möchten, dass Kaspersky Security Center Linux automatisch Programme deinstalliert, die mit dem zu verteilenden Programm inkompatibel sind.

Die Liste der inkompatiblen Programme wird ebenfalls angezeigt.

Wenn Sie diese Option nicht auswählen, wird das Programm nur auf Geräten installiert, die keine inkompatiblen Programme aufweisen.

Schritt 8. 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.

Schritt 9. 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 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 angeben, um das Programm zu installieren.

  Um das Benutzerkonto anzugeben, unter dem das Installationsprogramm ausgeführt werden soll, klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Lokales Benutzerkonto** 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.

Schritt 10. Beginnen der Installation

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 15.1 des Administrationsservers auf einem Gerät installieren, auf dem eine ältere Version des Administrationsservers installiert ist (ab Version 13). Beim Aktualisieren auf die Version 15.1 bleiben alle Daten und Einstellungen der vorherigen Version des Administrationsservers erhalten.

Stellen Sie vor dem Upgrade von Kaspersky Security Center Linux sicher, dass Sie die Versionen des Betriebssystems und des DBMS verwenden, die vom Administrationsserver in Version 15.1 unterstützt werden. Bei Bedarf können Sie den Administrationsserver auf ein anderes Gerät mit aktuelleren Versionen des Betriebssystems und des DBMS verschieben.

Für das Upgrade einer Version des Administrationsservers gibt es die folgenden Methoden:

- Verwendung der Installationsdatei für Kaspersky Security Center Linux
- Erstellen eines Backups der Administrationsserver-Daten, 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.

Darüber hinaus müssen Sie Kaspersky Security Center Web Console auf eine neue Version aktualisieren.

Beachten Sie, dass Sie bei einer Aktualisierung des Administrationsservers auf Version 15.1 keine neuen Installationspakete des Administrationsagenten in Version 15 oder früher 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. Es wird empfohlen, vor dem Upgrade eine Backup-Kopie der Daten des Administrationsservers anzulegen.

Kaspersky Security Center Linux mittel Installationsdatei aktualisieren

Um den Administrationsserver von einer früheren Version (ab Version 13) auf Version 15.1 zu aktualisieren, können Sie mithilfe der Installationsdatei von Kaspersky Security Center Linux eine neue Version über eine frühere Version installieren.

Um den Administrationsserver von einer älteren Version auf die Version 15.1 upzugraden:

1. Laden Sie die Installationsdatei für Kaspersky Security Center Linux mit einem vollständigen Paket für Version 15.1 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. Upgraden Sie das Installationspaket mithilfe eines Paketmanagers, den Sie auf Ihrem Administrationsserver verwenden. Sie können beispielsweise die folgenden Befehle im Befehlszeilenterminal unter einem Benutzerkonto mit Root-Rechten verwenden:

   - Für Geräte mit einem RPM-basiertem Betriebssystem:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<Versionsnummer>.x86_64.rpm
     ```
   - Für Geräte mit einem Debian-basiertem Betriebssystem:
     ```
     $ sudo dpkg -i ksc64_<Versionsnummer>_amd64.deb
     ```

   Nachdem der Befehl erfolgreich ausgeführt wurde, wird das Skript /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl erstellt. Eine entsprechende Meldung wird im Terminal angezeigt.

3. Führen Sie unter einem Benutzerkonto mit Root-Berechtigung das Skript /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl aus, um den aktualisierten Administrationsserver zu konfigurieren.

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:

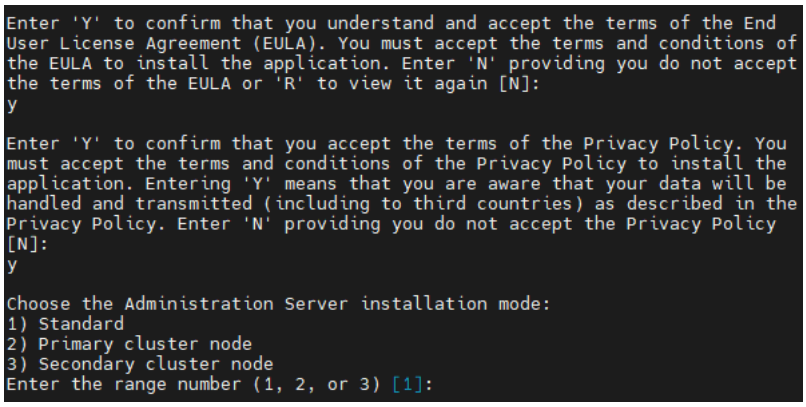
   a. Geben Sie "Y" ein, um zu bestätigen, dass Sie die Bedingungen der EULA vollständig gelesen und verstanden haben, und sie akzeptieren.

   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. 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.

Kaspersky Security Center Linux mittels Backup aktualisieren

Um den Administrationsserver von einer früheren Version (ab Version 13) auf Version 15.1 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.

Um den Administrationsserver über ein Backup von einer älteren Version auf die Version 15.1 upzugraden:

1. Erstellen Sie vor dem Upgrade ein Backup der Administrationsserver-Daten mit einer älteren Programmversion.
2. Deinstallieren Sie die ältere Version von Kaspersky Security Center Linux.
3. Installieren Sie Kaspersky Security Center Linux Version 15.1 auf dem bisherigen Administrationsserver.
4. Stellen Sie die Daten des Administrationsservers aus dem Backup, das vor dem Upgrade erstellt wurde, wieder her.
5. 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.

Kaspersky Security Center Linux auf den Knoten des Kaspersky Security Center Linux Failover-Clusters aktualisieren

Sie können den Administrationsserver in Version 15.1 auf jedem Knoten des Kaspersky Security Center Linux Failover-Clusters installieren, auf dem der Administrationsserver in einer früheren Version installiert ist (beginnend mit Version 14). Beim Aktualisieren auf die Version 15.1 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 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 15.1 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. Hängen Sie die freigegebenen Ordner für das Cluster aus und hängen Sie diese mit den Optionen wieder ein, die im Abschnitt Einen Dateiserver für ein Kaspersky Security Center Linux Failover-Cluster vorbereiten angegeben sind.

4. Ordnen Sie auf den Cluster-Knoten die Einhängepunkte und die freigegebenen Ordner erneut zu, wie im Abschnitt Knoten für ein Kaspersky Security Center Linux Failover-Cluster vorbereiten angegeben ist.

5. Aktualisieren Sie auf dem aktiven Knoten des Clusters das Installationspaket mithilfe eines Paketmanagers, den Sie auf Ihrem Administrationsserver verwenden.

   Sie können beispielsweise die folgenden Befehle im Befehlszeilenterminal unter einem Benutzerkonto mit Root-Rechten verwenden:

   - Für Geräte mit einem RPM-basiertem Betriebssystem:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc64-<Versionsnummer>-<Build-Nummer>.x86_64.rpm
     ```

   - Für Geräte mit einem Debian-basiertem Betriebssystem:
     ```
     $ sudo dpkg -i ksc64_<Versionsnummer>-<Build-Nummer>_amd64.deb
     ```

   Nachdem der Befehl erfolgreich ausgeführt wurde, wird das Skript /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl erstellt. Eine entsprechende Meldung wird im Terminal angezeigt.

6. Führen Sie unter einem Benutzerkonto mit Root-Berechtigung das Skript /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl aus, um den aktualisierten Administrationsserver zu konfigurieren.

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:

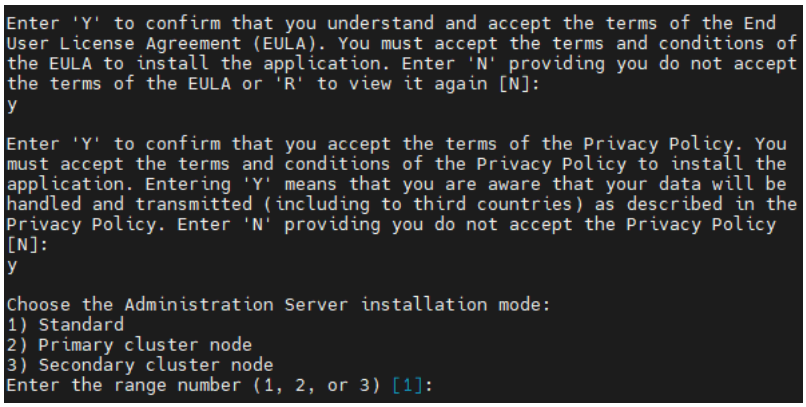
   a. Geben Sie "Y" ein, um zu bestätigen, dass Sie die Bedingungen der EULA vollständig gelesen und verstanden haben, und sie akzeptieren.

   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.



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.

9. Führen Sie die Schritte 3-5 auf dem passiven Knoten aus.

   Geben Sie in Schritt 6 eine "3" ein, um den Knoten auszuwählen.

10. Starten Sie das Cluster.

    Beachten Sie, dass Sie den Cluster auf jedem Knoten starten können. Wenn Sie den Cluster auf dem passiven Knoten starten, wird er zum aktiven Knoten.

    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 Kaspersky Security Center Web Console (auch als Kaspersky Security Center Web Console bezeichnet) 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, die der auf Ihrem Gerät installierten Linux-Distribution entspricht:

- Für Debian – ksc-web-console-[Build-Nummer].x86_64.deb
- Für RPM-basierte Betriebssysteme – ksc-web-console-[Build-Nummer].x86_64.rpm
- Für ALT 8 SP – ksc-web-console-[Build-Nummer]-alt8p.x86_64.rpm

Sie erhalten die Installationsdatei, indem Sie diese von der Kaspersky-Website herunterladen.

Um Kaspersky Security Center Web Console zu aktualisieren:

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 dieselbe 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" ab.

   Beispiel für eine Antwortdatei mit minimalem Parametersatz sowie Standardadresse und Standardport:

   ```
   {
     "address": "127.0.0.1",
     "port": "8080",
     "trusted":
     "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
     Server",
     "acceptEula": "true"
   }
   ```

   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 `vertrauenswürdigen` Installationsparameter an, damit der Kaspersky Security Center Linux-Failover-Cluster eine Verbindung mit der Kaspersky Security Center Web Console herstellen kann. Der Zeichenfolge dieses Parameters hat das folgende Format:

   ```
   "trusted": "Serveradresse|Port|Pfad des Zertifikats|Servername"
   ```

   Geben Sie die Komponenten der `vertrauenswürdigen` Installationsparameter an:

   - **Adresse des Administrationsservers**. Wenn Sie einen sekundären Netzwerkadapter im Rahmen der Vorbereitung der Cluster-Knoten erstellt haben, verwenden Sie die IP-Adresse des Adapters als Adresse für das Kaspersky Security Center Linux Failover-Cluster. Geben Sie andernfalls die IP-Adresse eines von Ihnen verwendeten Load Balancers eines Drittanbieters an.

   - **Port des Administrationsservers**. Der OpenAPI-Port, den Kaspersky Security Center Web Console für die Verbindung mit dem Administrationsserver verwendet (Standardwert ist 13299).

   - **Zertifikat des Administrationsservers**. Das Zertifikat des Administrationsservers befindet sich im freigegebenen Datenspeicher des Kaspersky Security Center Linux Failover-Clusters. Der Standardpfad zur Zertifikatsdatei lautet: <freigegebener Datenordner>\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.

   - **Name des Administrationsservers**. Der Name des Kaspersky Security Center Linux Failover-Clusters, der im Anmeldefenster der Kaspersky Security Center Web Console angezeigt 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 von einer früheren Version von Kaspersky Security Center Web Console zu aktualisieren, führen Sie einen der folgenden Befehle aus:

   - Für Geräte mit einem RPM-basiertem Betriebssystem:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc-web-console-[Build-Nummer].x86_64.rpm
     ```
   - Für Geräte mit einem Debian-basiertem Betriebssystem:
     ```
     $ sudo dpkg -i ksc-web-console-[Build-Nummer].x86_64.deb
     ```

   Dadurch wird die Installationsdatei entpackt. Bitte warten Sie, bis die Installation abgeschlossen ist.

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 Aktualisierung 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 Kaspersky Security Center Web Console (auch als Kaspersky Security Center Web Console bezeichnet) unter dem Betriebssystemen Astra Linux Special Edition aktualisieren.

Um Kaspersky Security Center Web Console zu aktualisieren:

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 dieselbe 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" ab.

   Beispiel für eine Antwortdatei mit minimalem Parametersatz sowie Standardadresse und Standardport:

   ```
   {
     "address": "127.0.0.1",
     "port": "8080",
     "trusted":
   "127.0.0.1|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
     "acceptEula": "true"
   }
   ```

4. Stellen Sie sicher, dass in der Datei `/etc/digsig/digsig_initrafs.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 Programmschlüssel "/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg" in das Verzeichnis ab, das Sie im vorherigen Schritt erstellt haben:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Wenn der Programmschlüssel "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 Installationsdatei auszuführen. Sie können die Installationsdatei von der Kaspersky-Website herunterladen.

   Um von einer früheren Version von Kaspersky Security Center Web Console zu aktualisieren, führen Sie den folgenden Befehl aus:

   ```
   $ sudo dpkg -i ksc-web-console-[Build-Nummer].x86_64.deb
   ```

   Dadurch wird die Installationsdatei entpackt. Bitte warten Sie, bis die Installation abgeschlossen ist.

10. 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 Aktualisierung können Sie in Ihrem Browser die Adresse von Kaspersky Security Center Web Console aufrufen und sich anmelden.

Migration nach Kaspersky Security Center Linux

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 von Kaspersky Security Center 14.2 Windows ist nur auf Kaspersky Security Center Linux ab Version 15 möglich.
- Dieses Szenario kann nur über die Kaspersky Security Center Web Console ausgeführt 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 Programmen von Kaspersky, 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 von 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 von Kaspersky Security Center Windows als sekundärer Administrationsserver von 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 von 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. **Daten aus Kaspersky Security Center Windows exportieren**

   Öffnen Kaspersky Security Center Windows und starten Sie anschließend den Migrationsassistenten.

3. **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.

4. **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
   - Verteilungspunkte zuweisen und konfigurieren
   - Regeln für das Verschieben von Geräten konfigurieren
   - Regeln für das automatische Zuweisen von Tags an Geräte konfigurieren
   - Programmkategorien erstellen

5. **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. In der aktuellen Version von Kaspersky Security Center Linux können Sie dies auf eine der folgenden Weisen tun:

   - Mithilfe des Tools klmover.

     Verwenden Sie das Tool "klmover" und geben Sie die Verbindungseinstellungen des neuen Administrationsservers an.

   - Mittels Installation oder Neuinstallation 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. Verwenden Sie das Installationspaket, um den Administrationsagenten mit einer Aufgabe zur Remote-Installation auf den importierten verwalteten Geräten zu installieren. Weitere Informationen finden Sie unter Verwaltete Geräte unter die Verwaltung von Kaspersky Security Center Linux stellen.

     Sie können auch ein autonomes Installationspaket erstellen und den Administrationsagenten mittels des Pakets lokal installieren.

6. **Administrationsagent auf die neueste Version aktualisieren**

   Es wird empfohlen, den Administrationsagenten für Linux auf dieselbe Version zu aktualisieren, wie Kaspersky Security Center.

7. **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 (**Assets (Geräte)** → **Verwaltete 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 Methoden 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 Programme
- 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 allgemeine Informationen zur Migration auf Kaspersky Security Center Linux vertraut. Wählen Sie die Migrationsmethode – mit oder ohne Verwendung der Hierarchie der Administrationsserver von 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 Administrationsserver von 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. Wechseln 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 Programme aus, deren Aufgaben und Richtlinien exportiert werden. Wählen Sie nur Programme aus, die auch von Kaspersky Security Center Linux unterstützt werden. Die Objekte von nicht unterstützten Programmen 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 von Kaspersky Security Center Web Console Server 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 die Kaspersky Security Center Linux oder Kaspersky 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 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 **Assets (Geräte)** 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.

In der aktuellen Version von Kaspersky Security Center Linux können Sie die verwalteten Geräte unter Verwaltung von Kaspersky Security Center Linux stellen, indem Sie entweder das Tool klmover verwenden, oder indem Sie auf den verwalteten Geräten den Administrationsagenten mittels Aufgabe zur Remote-Installation installieren.

So stellen Sie die verwalteten Geräte mithilfe der Installation des Administrationsagenten unter Verwaltung von Kaspersky Security Center Linux:

1. Wechseln Sie zum Administrationsserver von Kaspersky Security Center Windows.

2. Gehen Sie zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → 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.

3. Wählen Sie auf der Registerkarte **Einstellungen** den Abschnitt **Verbindung**. Geben Sie die Verbindungseinstellungen für den Administrationsserver von Kaspersky Security Center Linux an.

4. 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 von 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**.

5. Starten Sie die Aufgabe zur Remote-Installation des Programms.

Nachdem die Aufgabe zur Remote-Installation erfolgreich abgeschlossen wurde, wechseln Sie zum Administrationsserver von 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.

Verbindung zwischen Kaspersky Security Center Web Console und Administrationsserver anpassen

So legen Sie die Verbindungsports des Administrationsservers fest:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **Verbindungsports** aus.

Die Anwendung zeigt die wichtigsten Verbindungseinstellungen des ausgewählten Servers an.

Allow-Liste mit IP-Adressen für die Anmeldung bei Kaspersky Security Center Linux konfigurieren

Standardmäßig können sich Benutzer auf jedem Gerät, auf dem sie die Kaspersky Security Center 14 Web Console öffnen können, bei Kaspersky Security Center Linux anmelden. Sie können den Administrationsserver jedoch auch so konfigurieren, dass Benutzer nur von Geräten mit zugelassenen IP-Adressen eine Verbindung zu ihm herstellen dürfen. Selbst wenn ein Eindringling an die Anmeldedaten eines Benutzerkontos von Kaspersky Security Center Linux gelangt, kann er sich in diesem Fall nicht bei Kaspersky Security Center Linux anmelden, da die IP-Adresse des Geräts des Eindringlings nicht auf der Allow-Liste steht.

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 das Gerät des Benutzers, 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 Programme versuchen, sich mit dem Administrationsserver zu verbinden:

- Server der Kaspersky Security Center Web Console

  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 Kaspersky Security Center Web Console installiert ist. Wenn anschließend jemand versucht, sich von einem Gerät aus an Kaspersky Security Center Linux anzumelden, wobei der Server der Kaspersky Security Center Web Console auf einem anderen Gerät installiert ist, hilft eine Firewall, die Eindringlinge abzuweisen.

- Programme, die mittels klakaut-Automatisierungsobjekten mit dem Administrationsserver interagieren
- Programme, 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 Programme 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 Zulassungsliste 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-Programme herunterzuladen.

So geben Sie die Internetzugriffseinstellungen für den Administrationsserver an:

1. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol () neben dem 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.

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. Klicken Sie auf dem zukünftigen primären Administrationsserver auf das Einstellungen-Symbol ( ).
3. Wechseln Sie auf der folgenden Eigenschaftenseite 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.

   Stellen Sie sicher, dass die zweistufige Überprüfung für das angegebene Konto deaktiviert ist. Wenn die zweistufige Überprüfung für dieses Konto aktiviert ist, können Sie die Hierarchie nur vom zukünftigen sekundären Server erstellen (siehe Anweisungen unten). Das ist ein bekanntes Problem.

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 das Einstellungen-Symbol ( ).

   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:

Klicken Sie im Hauptmenü auf den Namen des Administrationsservers neben dem Einstellungen-Symbol ( ).

Eine Dropdown-Liste mit sekundären (einschl. virtuellen) Administrationsservern wird angezeigt.

Sie können auf den Namen eines dieser Administrationsserver klicken, um zu ihm zu wechseln.

Die Administrationsgruppen werden ebenfalls angezeigt, sind jedoch ausgegraut und stehen in diesem Menü nicht zur Verwaltung zur Verfügung.

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 des Programms 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.

Um einen virtuellen Administrationsserver zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).
2. Wechseln 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.
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 des Programms 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

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 zu "Aktiviert" oder "Deaktiviert". Der aktualisierte Status wird nehmen 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 im Hauptmenü zum erforderlichen virtuellen Administrationsserver:
   a. Klicken Sie rechts neben dem Namen des aktuellen Administrationsservers auf das Chevron-Symbol ( ).
   b. Wählen Sie den gewünschten Administrationsserver aus.
2. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.
   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.

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 im Hauptmenü zum erforderlichen virtuellen Administrationsserver:

   a. Klicken Sie rechts neben dem Namen des aktuellen Administrationsservers auf das Chevron-Symbol (▸).

   b. Wählen Sie den gewünschten Administrationsserver aus.

3. Weisen Sie die neue Rolle oder mehrere Rollen dem Administratorkonto zu.

Das Programm 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

Sie können den Administrationsserver, der die Client-Geräte verwaltet, durch einen anderen Administrationsserver mit der Aufgabe **Administrationsserver wechseln** ersetzen. Nach Abschluss der Aufgabe werden die Client-Geräte unter die Verwaltung des Administrationsservers gestellt, denn Sie angegeben haben.

Um einen Administrationsserver, der die Client-Geräte verwaltet, zu wechseln, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
3. Wählen Sie für Kaspersky Security Center den Aufgabentyp **Administrationsserver wechseln**.
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 den Administrationsserver aus, den Sie für die Verwaltung der ausgewählten Geräte verwenden möchten.
7. Legen Sie die Benutzerkonto-Einstellungen fest:

   - **Standardbenutzerkonto**

     Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, unter dem das Programm installiert und gestartet wurde, dass diese Aufgabe ausführt.

     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 dessen Namen die Aufgabe ausgeführt wird.

   - **Kennwort**

     Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.
8. Wenn Sie auf der Seite **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.
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 entsprechend Ihrer Bedürfnisse 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 alle Objekte, die auf dem virtuellen Administrationsserver erstellt wurden, inklusive Richtlinien und Aufgaben ebenfalls gelöscht. Die verwalteten Geräte aus den Administrationsgruppen, die von dem virtuellen Administrationsserver verwaltet wurden, werden von 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 von der Gruppe "Nicht zugeordnete Geräte" in die Administrationsgruppe verschieben.

So löschen Sie einen virtuellen Administrationsserver:

1. Klicken Sie im Hauptmenü auf das Einstellungen-Symbol ( ) neben dem Namen des Administrationsservers.

2. Wechseln Sie auf der nächsten Seite auf die Registerkarte **Administrationsserver**.

3. Wählen Sie den virtuellen Administrationsserver aus, den Sie löschen möchten.

4. Klicken Sie auf der Menüleiste auf die Schaltfläche **Löschen**.

Der virtuelle Administrationsserver wurde gelöscht.

Protokoll der Verbindungen zum Administrationsserver anzeigen

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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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 Datenbank des Servers 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 Datenbank des Administrationsservers 400.000 Ereignisse. Die empfohlene Maximalgröße der Datenbank liegt bei 45 Millionen Ereignissen.

Das Programm überprüft die Datenbank alle 10 Minuten. Wenn die Anzahl der Ereignisse den festgelegten Höchstwert plus 10.000 erreicht, löscht das Programm 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 dieser Zeitspanne 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. So begrenzen Sie die Anzahl der Ereignisse, die in der Ereignisverwaltung auf dem Administrationsserver gespeichert werden können:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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**.

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.
- Belassen Sie den Datenbankserver auf dem bisherigen Gerät und verschieben Sie nur den Administrationsserver auf ein neues Gerät.

Um den Administrationsserver und den Datenbankserver auf ein neues Gerät zu verschieben:

1. Erstellen Sie auf dem bisherigen Gerät ein Backup der Daten des Administrationsservers.

   Dazu können Sie entweder die Datensicherungsaufgabe über Kaspersky Security Center Web Console ausführen oder das Dienstprogramm klbackup ausführen.

2. 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.

3. Installieren Sie auf dem neuen Gerät das DBMS, das vom Administrationsserver verwenden wird.

   Berücksichtigen Sie bei der Auswahl eines DBMS die Anzahl der vom Administrationsserver verwalteten Geräte.

4. Installieren Sie den Administrationsserver auf dem neuen Gerät.

   Hinweis: Wenn Sie den Datenbankserver auf das neue Gerät verschieben, müssen Sie die lokale Adresse als IP-Adresse des Gerätes angeben, auf dem die Datenbank installiert ist (Element "h" in der Anweisung Kaspersky Security Center Linux installieren). 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.

5. Stellen Sie nach Abschluss der Installation die Administrationsserver-Daten auf dem neuen Gerät mithilfe des Tools "klbackup" wieder her.

6. Öffnen Sie die Kaspersky Security Center Web Console und stellen Sie eine Verbindung zum Administrationsserver her.

7. Überprüfen Sie, ob alle Client-Geräte mit dem Administrationsserver verbunden sind.

8. 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.

Um die DBMS-Anmeldedaten in einer Linux-Umgebung mithilfe des Dienstprogramms klsrvconfig zu ändern:

1. Starten Sie eine Linux-Befehlszeile.

2. Geben Sie im angezeigten Befehlszeilenfenster das Dienstprogramm klsrvconfig an:

   ```
   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.

Die DBMS-Anmeldeinformationen werden geändert.

Backup-Kopie der Daten des Administrationsservers anlegen und wiederherstellen

Das Anlegen eines Backups ermöglicht es Ihnen, den Administrationsserver ohne Datenverlust von einem Gerät auf ein anderes zu übertragen. Mithilfe des Backups können Sie Daten wiederherstellen, wenn die Datenbank des Administrationsservers auf ein anderes Gerät verschoben wird oder wenn auf eine aktuellere Version von Kaspersky Security Center Linux aktualisiert wird (Das Verschieben der Daten des Administrationsservers unter die Verwaltung von Kaspersky Security Center Windows wird nicht unterstützt).

Beachten Sie, dass die installierten Verwaltungs-Plug-Ins nicht gesichert werden. Nachdem Sie die Daten des Administrationsservers aus einer Sicherungskopie wiederhergestellt haben, müssen Sie Plug-ins für die verwalteten Programme herunterladen und neu installieren.

Bevor Sie ein Backup des Administrationsservers erstellen, prüfen 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.

Sie können eine Backup-Kopie der Daten des Administrationsservers auf eine der folgenden Weisen erstellen:

- Erstellen und Ausführen einer Datensicherungsaufgabe 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 Programm-Installation angegeben wurde (gewöhnlich im Ordner /opt/kaspersky/ksc64/sbin/klbackup).

In der Backup-Kopie der Daten des Administrationsservers werden folgende Daten gespeichert:

- Datenbank des Administrationsservers (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.

Die Wiederherstellung von Daten des Administrationsservers ist nur mithilfe des Hilfsprogramms klbackup möglich.

Sicherungsaufgabe für die Daten des Administrationsserver erstellen

Sicherungsaufgaben gehören zu den Aufgaben des Administrationsservers und werden vom 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 Backup-Aufgabe für die Daten des Administrationsservers für den Administrationsserver bereits erstellt wurde, wird sie im Fenster für die Auswahl des Aufgabentyps nicht angezeigt.

Um eine Aufgabe zum Anlegen eines Backups des Administrationsservers zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **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 **Programm** die Option **Kaspersky Security Center 15** 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.

Wenn Sie in Kaspersky Security Center Linux 15.0 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.

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_PATH [-logfile LOGFILE] [-use_ts]|[-restore] [-password PASSWORD]
[-cert_only] [-online]
```

Wenn in der Befehlszeile des Tools klbackup kein Kennwort eingegeben wird, fragt das Tool das Kennwort interaktiv ab.

Die Schlüssel weisen folgende Bedeutung auf:

- `-path BACKUP_PATH` – Daten im Ordner BACKUP_PATH speichern/zum Wiederherstellen Daten aus dem Ordner BACKUP_PATH (Pflichtparameter) verwenden.

- `-logfile LOGFILE` – Bericht über das Kopieren oder Wiederherstellen der Daten des Administrationsservers speichern.

  Das Benutzerkonto der Server-Datenbank und das Tool klbackup müssen über die Berechtigung zum Ändern der Daten im Ordner BACKUP_PATH verfügen.

- `-use_ts` – Beim Speichern die Daten in einen Unterordner im Ordner BACKUP_PATH kopieren, dessen Name das aktuelle Systemdatum und die aktuelle Systemuhrzeit im Format `klbackup JJJJ-MM-TT # HH-MM-SS` enthält. Wenn der Schlüssel nicht eingegeben wurde, werden die Angaben im Stammverzeichnis des Ordners BACKUP_PFAD 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 `C:\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 im Ordner BACKUP_PFAD liegen. Wenn der Schlüssel fehlt, wird die Backup-Kopie im Ordner BACKUP_PATH erstellt.

- `-password PASSWORD` – Zertifikat des Administrationsservers speichern oder wiederherstellen. Für die Verschlüsselung und Entschlüsselung des Zertifikats wird das Kennwort verwendet, das mit dem Parameter PASSWORD vorgegeben wurde.

  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` – Das Zertifikat und den privaten Schlüssel des Administrationsservers nur speichern oder wiederherstellen.

- `-online` – Daten des Administrationsservers mithilfe der Erstellung eines Volume-Snapshots sichern, um die Offline-Zeit des Administrationsservers zu reduzieren. Dieser Parameter ist nicht obligatorisch.

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 SQL Server oder PostgreSQL als DBMS):
  - Die Datenbank wird auf Fehler geprüft (nur SQL Server).
  - 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 **Assets (Geräte)** → **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 neben dem Namen des primären Administrationsservers auf das Einstellungen-Symbol ( ).
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 das Programm 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. Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **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 aktivieren Wenn Sie **Alarme von EDR anzeigen** anzeigen , erscheint im Hauptmenü der Abschnitt **Überwachung und Berichterstattung** → **Alarme** (stellen Sie zunächst sicher, dass Sie einen Lizenzschlüssel für EDR Optimum hinzufügen um Informationen über erkannte Bedrohungen auf den Endgeräten anzuzeigen).

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.

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.

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

Bei der Schnellabfrage empfängt der Administrationsserver nur Informationen über die Liste der NetBIOS-Namen der Geräte aller Domänen und Arbeitsgruppen des Netzwerks. 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.

Einstellungen der Windows-Netzwerkabfrage anzeigen und ändern

Um die Einstellungen der Windows-Netzwerkabfrage zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur aus dem Ordner **Gerätesuche** den Unterordner **Domänen**.

   Sie können zum Ordner **Gerätesuche** aus dem Ordner **Nicht zugeordnete Geräte** wechseln, indem Sie auf die Schaltfläche **Jetzt abfragen** klicken.

   Im Arbeitsbereich des Unterordners **Domänen** wird eine Liste mit Geräten angezeigt.

2. Klicken Sie auf die Schaltfläche **Jetzt abfragen**.

   Das Fenster der Domäneneigenschaften wird geöffnet. Bearbeiten Sie bei Bedarf die Einstellungen der Windows-Netzwerkabfrage:

   - **Abfrage des Windows-Netzwerks aktivieren**

     Diese Variante ist standardmäßig festgelegt. Wenn Sie keine Windows-Netzwerkabfrage durchführen möchten (z. B. weil die Abfrage des Active Directory für Sie ausreichend ist), können Sie diese Option deaktivieren.

   - **Zeitplan für schnelle Abfrage festlegen**

Das Standardintervall beträgt 15 Minuten.

Bei der Schnellabfrage empfängt der Administrationsserver nur Informationen über die Liste der NetBIOS-Namen der Geräte aller Domänen und Arbeitsgruppen des Netzwerks.

Alte Daten werden vollständig durch die bei der nächsten Abfrage empfangenen Daten 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.

  Standardmäßig wird die Abfrage ab der aktuellen Systemzeit alle fünf Minuten ausgeführt.

- **Nach Wochentagen**

  Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

  Die Abfrage wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.

- **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 aktiviert.

- **Zeitplan für vollständige Abfrage festlegen**

Das Standardabfrageintervall beträgt eine Stunde. Alte Daten werden vollständig durch die bei der nächsten Abfrage empfangenen Daten 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.

  Standardmäßig wird die Abfrage ab der aktuellen Systemzeit alle fünf Minuten ausgeführt.

- **Nach Wochentagen**

  Die Abfrage wird regelmäßig an den festgelegten Wochentagen und zur festgelegten Uhrzeit ausgeführt.

  Die Abfrage wird standardmäßig jeden Freitag um 18:00:00 Uhr ausgeführt.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Abfrage wird regelmäßig an den festgelegten Tagen des Monats und zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig sind keine Tage des Monats ausgewählt; die Standardstartzeit ist 18:00:00 Uhr.

- **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 aktiviert.

Wenn Sie die Abfrage sofort durchführen möchten, klicken Sie auf **Jetzt abfragen**. Beide Arten der Abfrage werden gestartet.

Am virtuellen Administrationsserver können Sie im Eigenschaften-Fenster des Verteilungspunkts im Abschnitt **Gerätesuche** die Einstellungen für die Windows-Netzwerkabfrage anzeigen und ändern.

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 dem Befehl "ping") 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.

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. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → IP-Bereiche**.
2. Klicken Sie auf die Schaltfläche **Eigenschaften**.

   Das Eigenschaftenfenster der IP-Abfrage wird geöffnet.
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, an angegebenen Tagen der gewählten Wochen**

  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.

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. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Gerätesuche → 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.
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. Wechseln 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. Wechseln 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 eines Microsoft Active Directory-Domänencontrollers und eines Samba-Domänencontrollers. 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 die folgenden Ports auf dem Gerät des Domänencontrollers verfügbar sind:

- 389 für das LDAP-Protokoll und Simple Authentication (einschließlich SASL)
- 636 für das LDAPS-Protokoll

Abfrage des Domänencontrollers mithilfe des Administrationsservers

So fragen Sie einen Domänencontroller mithilfe des Administrationsservers ab:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung** → **Gerätesuche** → **Domänencontroller**.
2. Klicken Sie auf **Abfrage-Einstellungen**.

   Das Fenster **Einstellungen für die Abfrage des Domänencontrollers** wird geöffnet.
3. Wählen Sie die Option **Abfrage des Domänencontrollers aktivieren** aus.
4. Klicken Sie unter **Angegebene Domänen abfragen** auf **Hinzufügen** und geben Sie anschließend die Adresse und die Anmeldeinformationen des Domänencontrollers an.
5. Geben Sie bei Bedarf im Fenster **Einstellungen für die Abfrage des Domänencontrollers** 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, an angegebenen Tagen der gewählten Wochen

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 die Abfrage eines Microsoft Active Directory-Domänencontrollers und eines Samba-Domänencontrollers unterstützt.
Für einen Windows-Verteilungspunkt wird nur die Abfrage eines Microsoft Active Directory-Domänencontrollers unterstützt.
Die Abfrage 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. Wählen Sie die Option **Abfrage des Domänencontrollers aktivieren** aus.
4. 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**

5. 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

Bei der erstmaligen Verbindung mit dem Domänencontroller identifiziert der Administrationsserver das Verbindungsprotokoll. Dieses Protokoll wird für alle zukünftigen Verbindungen zum Domänencontroller verwendet.

Die erstmalige Verbindung mit einem Domänencontroller erfolgt folgendermaßen:

1. Der Administrationsserver versucht, über TLS eine Verbindung zum Domänencontroller herzustellen.

   Standardmäßig ist keine Überprüfung des Zertifikats notwendig. Um die Überprüfung des Zertifikats zu erzwingen, setzen Sie den Parameter "KLNAG_LDAP_TLS_REQCERT" auf 1.

   Standardmäßig wird für den Zugriff auf die Zertifikatskette der vom Betriebssystem abhängige Pfad zur Zertifizierungsstelle (CA) verwendet. Um einen benutzerdefinierten Pfad anzugeben, verwenden Sie den Parameter "KLNAG_LDAP_SSL_CACERT".

2. Wenn die TLS-Verbindung fehlschlägt, versucht der Administrationsserver, über SASL (DIGEST-MD5) eine Verbindung zum Domänencontroller herzustellen.

3. Wenn die SASL-Verbindung (DIGEST-MD5) fehlschlägt, verwendet der Administrationsserver Simple Authentication über eine unverschlüsselte TCP-Verbindung, um eine Verbindung mit dem Domänencontroller herzustellen.

Sie können das Tool "klscflag" verwenden, um die Parameter zu konfigurieren.

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".
Der folgende beispielhafte Befehl erzwingt die Überprüfung des Zertifikats:

```
klscflag -fset -pv klserver -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.

Wenn Sie einen Samba-Domänencontroller korrekt abfragen möchten, müssen Sie die Parameter `netbios name` und `workgroup` in der Datei `/etc/samba/smb.conf` angeben.

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 Datenbank des Administrationsservers 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 Datenbank des Administrationsservers 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 **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → 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. Wechseln Sie zu **Assets (Geräte) → 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**.

Beste Vorgehensweisen für die Softwareverteilung

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 – das grundlegende Tool für den Administrator. Sie können Kaspersky Security Center Web Console entweder auf demselben Gerät installieren, auf dem der Administrationsserver installiert ist, oder auf einem anderen Gerät.
- Administrationsagent – dient zur Verwaltung der auf dem Gerät installierten Sicherheitsanwendung sowie zum Empfangen von Informationen über das Gerät und zum Übertragen dieser Informationen an den Administrationsserver. 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 auf dem Gerät des Administrators
- Installation des Administrationsagenten und der Sicherheitsanwendung auf den Geräten des Unternehmens

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-Programmen 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.

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

Der Leitfaden zur Härtung 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 Programme von Drittanbietern
- Sicherheitsempfehlungen für Informationssysteme von Drittanbietern

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, in der folgendes berücksichtigt wird:

- 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 Programme von Drittanbietern installiert ist, 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 Datenbank des Administrationsservers aufgrund bekannter Schwachstellen kompromittiert wird.

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

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

Standardmäßig können sich Benutzer auf jedem Gerät, auf dem Kaspersky Security Center Web Console installiert ist, 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.

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.

Konten und Authentifizierung

Verwendung der zweistufigen Überprüfung mit dem Administrationsserver

Kaspersky Security Center Linux bietet eine zweistufige Überprüfung für Benutzer der Kaspersky Security Center Web Console. Diese basiert auf dem RFC 6238-Standard (TOTP: Time-Based One-Time Password Algorithm).

Wenn die zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktiviert ist, müssen Sie bei jeder Anmeldung an der Kaspersky Security Center Web Console den Benutzernamen, das Kennwort und einen zusätzlichen Einmal-Sicherheitscode eingegeben. Um einen Einmal-Sicherheitscode zu erhalten, müssen Sie auf einem Ihrer Geräte (z. B. auf Ihrem Computer oder mobilen Gerät) eine Authenticator-App 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

Für die Authentifizierung auf dem Gerät des Administrationsservers empfehlen wir die Verwendung der Multi-Faktor-Authentifizierung (MFA) mithilfe eines Tokens, einer Smartcard oder einer anderen Methode (falls möglich).

Verbieten der Speicherung des Administratorpassworts

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 folgende Regeln einhalten:

- Das Kennwort muss zwischen 8 und 256 Zeichen lang sein
- Das Kennwort muss Zeichen aus zumindest drei der unten aufgelisteten Gruppen enthalten:
  - Großbuchstaben (A–Z)
  - Kleinbuchstaben (a–z)
  - Zahlen (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.

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 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 Software von Drittanbietern 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 eine Rolle zuweisen oder Berechtigungen zuweisen.

Regelmäßige Überprüfung aller Benutzer

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.

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 Drittsoftware, die auf dem Gerät mit dem Administrationsserver installiert, 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-Software und Kaspersky-Programmen 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.

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 for 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. Bei der Installation des Administrationsagenten auf dem Client-Gerät wird das Tool automatisch in den Installationsordner des Administrationsagenten kopiert.

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. Für Geräte, die ohne lokale Administratorrechte betrieben werden, kann der Kennwortschutz für die Ausführung des Tools "klmover" ausgelassen werden.

Das Aktivieren der Option **Deinstallationskennwort verwenden** aktiviert 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 Gerätekontrolle: 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

Eine Datensicherung ermöglicht die Wiederherstellung der Daten des Administrationsservers ohne Datenverlust.

Standardmäßig wird nach der Installation des Administrationsservers automatisch eine Aufgabe zur Datensicherung erstellt und regelmäßig ausgeführt, wobei Sicherungen im entsprechenden Verzeichnis gespeichert werden.
Der Einstellungen des Aufgabe zur Datensicherung 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 Datenbank des Administrationsservers 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 auf Fehler überprüfen
- Datenbanken neu indizieren
- Datenbankstatistik aktualisieren
- Datenbank komprimieren (falls erforderlich)

Betriebssystem-Updates und Software-Updates von Drittanbietern installieren

Wir empfehlen dringend, auf dem Gerät mit dem Administrationsserver regelmäßig Software-Updates für das Betriebssystem und für die Software von Drittanbietern 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 Programme von Kaspersky 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 Informationssysteme von Drittanbietern

Sicherheitsempfehlungen der CIS-Benchmarks

Wenn Sie die vom Administrationsserver und vom Administrationsagenten unterstützten Versionen der Betriebssysteme, Virtualisierungsplattformen oder Datenbankserver einsetzen, empfehlen wir, für eine feinere Konfiguration dieser Informationssysteme die empfohlenen Verfahren für mehr Informationssicherheit des Center for Internet Security (CIS) (sofern vorhanden) anzuwenden.

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 CIPS-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:
  - 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 (in Russisch) beschrieben sind.

Sicherheitsempfehlungen für das Betriebssystem RED OS

Wenn Sie das Betriebssystem RED OS verwenden, sollten Sie die Sicherheitsempfehlungen befolgen, die in der offiziellen Dokumentation zu RED OS (in Russisch) beschrieben sind.

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 zur Datei 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 zur Datei ca-cert.pem> -t
   d

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <Pfad zur Datei server-
   cert.pem> -t d

   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <Pfad zur Datei server-
   key.pem> -t d
   ```

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

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

   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 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"
```

Szenario: Authentifizierung von PostgreSQL-Server

Es wird empfohlen, für die Authentifizierung am PostgreSQL-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 PostgreSQL sowohl die unidirektionale als auch die bidirektionale SSL-Authentifizierung.

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

1. **Generieren Sie ein Zertifikat 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 Sie ein Zertifikat 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 Sie die 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. **Geben Sie das PostgreSQL-Zertifikat an.**

   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. **Starten Sie den PostgreSQL-Daemon neu.**

   Führen Sie den folgenden Befehl aus:

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

6. **Geben Sie das Server-Flag für den Administrationsserver an.**

   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.

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <Pfad zur Datei psql.crt> -t d
   ```

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

   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.

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

   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 d
   ```

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

7. **Starten Sie den Dienst des Administrationsservers neu.**

Vorbereitung der Bereitstellung

In diesem Abschnitt werden Maßnahmen beschrieben, die Sie unternehmen müssen, bevor Sie mit der Bereitstellung von Kaspersky Security Center Linux beginnen.

Bereitstellung von Kaspersky Security Center Linux planen

Dieser Abschnitt informiert darüber, wie die Komponenten von Kaspersky Security Center Linux in einem Unternehmensnetzwerk in Abhängigkeit der folgenden Faktoren optimal bereitgestellt werden:

- 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

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-Programmen 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-Programmen 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®.

Über die Planung der Bereitstellung von Kaspersky Security Center Linux in einem Unternehmensnetzwerk

Ein Administrationsserver kann bis zu 20.000 Geräte unterstützen (mit MariaDB als DBMS). Wenn die Gesamtzahl der Geräte im Unternehmensnetzwerk 100.000 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; s. Abschnitt "Standard-Konfiguration: Wenige größere Büros werden jeweils von eigenen Administratoren verwaltet".

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 auch Abschnitt 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 Angabe der gewünschten Werte für die Felder des Zertifikats
- Zur Gewährleistung der erwünschten Verschlüsselungsstärke des Zertifikats

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 Konfigurationen von Kaspersky Security Center Linux

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 20.000 Geräte unterstützen (mit MariaDB 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. Beachten Sie dabei, dass die Verbindungsprofile des Administrationsagenten nur für Windows- und macOS-Geräte unterstützt werden.

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 entnehmen Sie folgendem Thema: Einen Push-Server aktivieren.

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.

Informationen zur Installation des ausgewählten DBMS finden Sie in dessen 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 MariaDB, PostgreSQL, oder Postgres Pro installieren, verwenden Sie die empfohlenen Einstellungen, um sicherzustellen, dass das DBMS ordnungsgemäß funktioniert.

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 Software von Drittanbietern

  Standardmäßig ist für den Administrationsserver keine Internetverbindung erforderlich, um Software-Updates von Microsoft auf den verwalteten Geräten zu installieren. Beispielsweise können die verwalteten Geräte die Software-Updates von Microsoft direkt von den Microsoft Update-Servern oder von Windows Server herunterladen, wobei Microsoft Windows Server Update Services (WSUS) im Netzwerk Ihres Unternehmens bereitgestellt werden. In den folgenden Fällen muss der Administrationsserver mit dem Internet verbunden sein:

  - Wenn Sie Administrationsserver als WSUS-Server verwenden
  - Um Updates anderer Drittanbieter-Software als Microsoft-Software zu installieren
- 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 Microsoft-Software. Die Liste wird von Kaspersky-Spezialisten erstellt und regelmäßig aktualisiert.
  - Beheben von Schwachstellen in anderer Software von Drittanbietern als Microsoft-Software.
- 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 des Unternehmens befindet, kann es hilfreich sein, den TCP-Port 13000 des Administrationsservers mithilfe der Portweiterleitung von außen erreichbar zu machen. Wenn die Verwaltung mobiler Geräte erforderlich ist, kann es hilfreich sein, den Port 13292 TCP erreichbar zu machen.

Zugriff aus dem Internet: Administrationsserver in der demilitarisierten Zone

Wenn sich der Administrationsserver in der demilitarisierten Zone des 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).

Zugriff aus dem Internet: Administrationsagent als Verbindungs-Gateway in der demilitarisierten Zone

Der Administrationsserver kann sich im internen Netzwerk der Organisation befinden, in dessen DMZ sich wiederum ein Gerät befindet, auf dem ein Administrationsagent als rückwärtsgerichtetes Verbindungs-Gateway ausgeführt wird (der Administrationsserver stellt eine Verbindung zum Administrationsagenten her). In diesem Fall müssen für die Organisation des Zugriffs aus dem Internet die folgenden Bedingungen erfüllt werden:

- Der Administrationsagent muss auf dem Gerät installiert werden, welches sich in der DMZ befindet. Wählen Sie bei der Installation des Administrationsagenten im Fenster **Verbindungs-Gateway** des Installationsassistenten den Punkt **Administrationsagent als Verbindungs-Gateway in der DMZ verwenden** aus.

- Das Gerät mit dem installierten Verbindungs-Gateway muss als Verteilungspunkt hinzugefügt werden. Wenn Sie das Verbindungs-Gateway in dem Fenster **Verteilungspunkt hinzufügen** angeben, wählen Sie die Option **Auswählen → Verbindungs-Gateway in DMZ mittels Adresse hinzufügen**.

- Um externe Desktop-Computer über eine Internetverbindung mit dem Administrationsserver zu verbinden, muss das Installationspaket für den Administrationsagenten angepasst werden. Wählen Sie in den Einstellungen des erstellten Installationspakets die Option **Advanced → Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen** und geben Sie anschließend das neu erstelle Verbindungs-Gateway an.

Für ein Verbindungs-Gateway, das sich in der demilitarisierten Zone befindet, erstellt der Administrationsserver ein Zertifikat, das vom Zertifikat des Administrationsservers signiert ist. Wenn der Administrator die Entscheidung gefasst hat, für den Administrationsserver das Benutzerzertifikat festzulegen, muss dies bis zum Erstellen des Verbindungs-Gateways in der demilitarisierten Zone erfolgen.

Wenn es Mitarbeiter mit Laptops gibt, die sich mit dem Administrationsserver sowohl aus dem lokalen Netzwerk als auch aus dem Internet verbinden, kann es zweckmäßig sein, in der Richtlinie des Administrationsagenten eine Regel zum Umschalten des Administrationsagenten zu erstellen.

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.

Anzahl der Datei-Deskriptoren für den klnagent-Dienst erhöhen

Wenn der Gültigkeitsbereich eines Linux-basierten Verteilungspunkts viele Geräte umfasst, ist die standardmäßige Beschränkung der Anzahl an öffenbaren Dateien (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. Öffnen Sie auf dem Linux-Gerät, das als Verteilungspunkt fungiert, die Datei `/lib/systemd/system/klnagent64.service` und geben Sie anschließend im Abschnitt `[Service]` die harten und weichen Beschränkungen der Datei-Deskriptoren mittels des Parameters `LimitNOFILE` an:

   `LimitNOFILE=<weiche Beschränkung>:<harte Beschränkung>`

   Beispiel: `LimitNOFILE=32768:131072`. Beachten Sie, dass die weiche Beschränkung der Datei-Deskriptoren kleiner oder gleich der harten Beschränkung sein muss.

2. 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: Parsen des Ressourcen-Werts ist fehlgeschlagen: 32768:13107`

     Wenn dieser Fehler auftritt, wurden die Zeichen in der Zeile `LimitNOFILE` falsch angegeben. Sie müssen die Syntax der eingegebenen Zeile überprüfen und korrigieren.

   - `/lib/systemd/system/klnagent64.service:11: Weiche Ressourcen-Beschränkung ist höher als harte Beschränkung. Ignoriere: 32768:13107`

     Wenn dieser Fehler auftritt, liegt die weiche Beschränkung der eingegebenen Datei-Deskriptoren über der harten Beschränkung. Sie müssen die eingegebene Zeile überprüfen und sicherstellen, dass die weiche Beschränkung der Datei-Deskriptoren kleiner oder gleich der harten Beschränkung ist.

3. Führen Sie den folgenden Befehl aus, um den Prozess "systemd" neu zu laden:

   ```
   systemctl daemon-reload
   ```

4. Führen Sie den folgenden Befehl aus, um den Dienst des Administrationsagenten neu zu starten:

   ```
   systemctl restart klnagent
   ```

5. Führen Sie den folgenden Befehl aus, um sicherzustellen, dass die angegebenen Parameter korrekt angewendet werden:

   ```
   less /proc/<nagent_proc_id>/limits
   ```

   wobei `<nagent_proc_id>` der Prozess-ID des Administrationsagenten entspricht. Um die Prozess-ID zu erfahren, können Sie den folgenden Befehl ausführen:

   ```
   ps -ax | grep klnagent
   ```

Für den Linux-basierten Verteilungspunkt wurde die Anzahl der Dateien erhöht, die geöffnet werden können.

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.

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

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	activation-v2.kaspersky.com/activationservice/activationservice.svc	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	Aktualisieren der Datenbanken, Softwaremodule und Anwendungen von Kaspersky

	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	
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.
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	Aktualisieren der Datenbanken, Softwaremodule und Anwendungen von Kaspersky

	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	
Port: 443 Protokoll: HTTPS	ds.kaspersky.com	Verwenden von Kaspersky Security Network
Port: 443, 1443 Protokoll: HTTPS	ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Verwenden von Kaspersky Security Network
Protokoll: HTTPS	click.kaspersky.com redirect.kaspersky.com	Folgen von Links aus der Benutzeroberfläche
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 den 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

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
     ```

Softwareverteilung für den Administrationsagenten und die Sicherheitsanwendung

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.

Unter Microsoft Windows XP führt der Administrationsagent möglicherweise die folgenden Vorgänge nicht korrekt aus: Updates direkt von den Kaspersky -Servern herunterladen (als Verteilungspunkt) und als KSN-Proxyserver agieren (als Verteilungspunkt).

Erstmalige Bereitstellung

Wenn auf einem Gerät der Administrationsagent schon installiert ist, erfolgt die Remote-Installation der Apps auf einem solchen Gerät mithilfe des Administrationsagenten. 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. Ausführliche Information über die Installation von Apps auf den verwalteten Geräten, auf denen der Administrationsagent schon installiert ist, finden Sie später in diesem Abschnitt.

Die erstmalige Installation des Administrationsagenten auf den Geräten auf der Microsoft Windows-Plattform kann auf folgende Arten erfolgen:

- Mithilfe von Dritthersteller-Tools zur Remote-Installation von Apps.
- Mittels Klonen eines Festplatten-Images mit dem Betriebssystem und dem installierten Administrationsagenten: durch von Kaspersky Security Center Linux für die Arbeit mit Laufwerks-Images bereitgestellten Tools oder Tools von Drittherstellern.
- Über den Mechanismus der Microsoft Windows-Gruppenrichtlinien: mithilfe der Standardtools zur Verwaltung von Microsoft Windows-Gruppenrichtlinien oder automatisiert, mithilfe der entsprechenden Option in der Aufgabe zur Remote-Installation in Kaspersky Security Center Linux.
- Erzwungen mithilfe der entsprechenden Optionen in der Aufgabe zur Remote-Installation von Kaspersky Security Center Linux.
- Mittels Versand eines Links auf die von Kaspersky Security Center Linux erstellten autonomen Pakete an die Benutzer der Geräte. Die autonomen Pakete stellen ausführbare Module dar, in denen die Programmpakete der ausgewählten Programme mit den konfigurierten Einstellungen enthalten sind.
- Manuell durch Starten der Installer der Programme auf den Geräten.

Auf anderen Plattformen als Microsoft Windows muss die erstmalige Installation des Administrationsagenten auf den verwalteten Geräten mithilfe der vorhandenen Dritthersteller-Tools erfolgen. Mithilfe der Aufgaben zur Remote-Installation von Apps und unter Verwendung von schon auf den Geräten vorhandenen Administrationsagenten können der Administrationsagent auf die neue Version aktualisiert und andere Apps von Kaspersky auf diesen Plattformen installiert werden. Die Installation erfolgt in diesem Fall analog zur Installation auf Geräten mit Microsoft Windows.

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 Active Directory-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.
- Zum Startzeitpunkt der Bereitstellung verwendete Sicherheitseinstellungen auf den Remote-Geräten (insbesondere Nutzung von UAC und des Modus Simple File Sharing).

Anpassen der Einstellungen der Installer

Vor Beginn der Bereitstellung der Programme von Kaspersky im Netzwerk müssen die Installationseinstellungen festgelegt werden – jene Einstellungen bestimmen, die im Verlauf der Programminstallation angepasst werden. Bei der Installation des Administrationsagenten muss zumindest die Adresse für die Verbindung mit dem Administrationsserver und, wenn möglich, auch einige erweiterte Einstellungen festgelegt werden. Abhängig von der ausgewählten Installationsmethode können die Einstellungen auf verschiedenen Weisen festgelegt werden. Jedenfalls können die erforderlichen Einstellungen (bei der interaktiven Installation manuell auf dem ausgewählten Gerät) mithilfe der Benutzerschnittstelle des Installers festgelegt werden.

Diese Methode zur Konfiguration der Einstellungen eignet sich nicht für die Silent-Installation der Programme auf den Gruppen der Geräte. Im typischen Fall muss der Administrator die Einstellungswerte, die in Folge für die Silent-Installation auf den ausgewählten Geräten im Netzwerk verwendet werden können, zentralisiert angeben.

Installationspakete

Die erste und wichtigste Methode zur Konfiguration der Installationseinstellungen der Programme ist universell und kommt für alle Installationsmethoden in Frage: sowohl mithilfe von Kaspersky Security Center Linux als auch mithilfe der meisten Dritthersteller-Tools. Diese Methode bedingt das Erstellen der Installationspakete der Programme in Kaspersky Security Center Linux.

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.

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.

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 Tools von Drittherstellern

Bei Verwendung von Tools von Drittherstellern für das Aufzeichnen des Images des Geräts mit dem installierten Administrationsagenten muss eine der folgenden Methoden verwendet werden:

- Auf dem geeichten Gerät, den Dienst des Administrationsagenten anhalten und das Tool klmover mit dem Parameter -dupfix ausführen. Das Tool klmover ist Teil des Installationspakets des Administrationsagenten. Im Folgenden den Start des Dienstes des Administrationsagenten bis zum Ausführen der Operation zum Aufzeichnen des Images nicht zulassen.

- Gewährleisten, dass der Start des Tools klmover mit dem Parameter -dupfix vor (zwingende Voraussetzung) dem ersten Start des Dienstes des Administrationsagenten auf den Geräten beim ersten Start des Betriebssystems nach der Bereitstellung des Images erfolgt. 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 das Laufwerkklonen 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 Gerätename wurde geändert
   b. Das Gerät wurde neu gestartet
   c. Das Laufwerk klonen-Modus wurde deaktiviert

Laufwerk klonen-Modus mithilfe des Dienstprogramms 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 Windows-Befehlszeile den Befehl `klmover -cloningmode 1` ein.

   Der Administrationsagent schaltet in den Laufwerk klonen-Modus.
3. Um den aktuellen Status des Laufwerk klonen-Modus abzurufen, geben Sie in der Befehlszeile den Befehl `klmover -cloningmode` ein.

   Im Fenster des Dienstprogramms wird angezeigt, ob der Laufwerk klonen-Modus aktiviert oder deaktiviert ist.
4. Um den Laufwerk klonen-Modus zu deaktivieren, geben Sie in der Dienstprogramm-Befehlszeile den Befehl `klmover -cloningmode 0` ein.

Erzwungene Bereitstellung mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center Linux

Falls es erforderlich ist, die Bereitstellung der Administrationsagenten oder anderer erforderlicher Apps sofort, ohne Abwarten der nächsten Anmeldung der Geräte in der Domäne zu starten, oder wenn Geräte vorhanden sind, die nicht Mitglieder der Domäne Active Directory sind, kann eine zwangsweise (erzwungene) Installation der ausgewählten Installationspakete mithilfe der Aufgabe zur Remote-Installation der Apps von Kaspersky Security Center Linux verwendet werden.

Die Geräte können dabei offen (über eine Liste) entweder durch Auswahl der Administrationsgruppe Kaspersky Security Center Linux, zu der sie gehören oder durch Erstellen einer Geräteauswahl nach einer bestimmten Bedingung angegeben werden. 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.

Diese Installationsmethode wird mittels Kopieren der Dateien auf die Administratorressource (admin$) der jeweiligen Geräte und der Remote-Anmeldung der Hilfsdienste auf ihnen ausgeführt. Nur festgelegte Verteilungspunkte können eine erzwungene Bereitstellung auf Windows-Geräten über die Verwaltungsressource ausführen. Dabei müssen die folgenden Bedingungen erfüllt werden:

- Die Geräte müssen für die Verbindung entweder seitens des Administrationsservers oder seitens des Verteilungspunkts verfügbar sein.
- Im Netzwerk muss die Namensauflösung für die Geräte korrekt arbeiten.
- Auf den verwalteten Geräten dürfen die freigegebenen Administratorressourcen (admin$) nicht deaktiviert sein.
- Auf den Geräten muss der Systemdienst Server gestartet worden sein (standardmäßig wird dieser Dienst gestartet).
- Auf den Geräten müssen die folgenden Ports für den Remote-Zugriff auf die Geräte mithilfe von Windows geöffnet sein: TCP 139, TCP 445, UDP 137, UDP 138.
- Auf den Geräten muss der Modus Simple File Sharing deaktiviert sein.
- Auf den Zielgeräten müssen sich das Modell für Freigabe und Sicherheit für die lokalen Benutzerkonten im Status *Normal – Lokale Benutzer authentifizieren sich als sie selbst* (Classic – local users authenticate as themselves) und keinesfalls im Status *Gast – Lokale Benutzer authentifizieren sich als Gäste* (Guest only – local users authenticate as Guest) befinden.
- Die Geräte müssen Mitglieder der Domäne sein oder auf den Geräten müssen rechtzeitig einheitliche Benutzerkonten mit Verwaltungsrechten erstellt worden sein.

Geräte, die sich in den Arbeitsgruppen befinden, können bei Erfüllung der obigen Anforderungen mithilfe des Tools "riprep" angegeben werden, das auf der Website des Technischen Supports von Kaspersky beschrieben ist.

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.

Es besteht die Möglichkeit, eine vereinfachte Methode zum Erstellen der Aufgaben zur erzwungenen Installation der Apps zu verwenden, nämlich die automatische Installation. Dazu müssen in den Eigenschaften der Administrationsgruppe in der Liste der Installationspakete jene Pakete ausgewählt werden, 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.

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. Damit die erzwungene Installation funktioniert, müssen in jedem isolierten Netzwerk Verteilungspunkte vorhanden sein.

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. Es muss jedoch berücksichtigt werden, dass diese Installationsmethode eine erhebliche Belastung für die Geräte darstellt, die als Verteilungspunkte agieren. Deshalb müssen als Verteilungspunkte Geräte ausgewählt werden, die ausreichend leistungsstark sind und einen schnellen Speicher aufweisen. Es ist ferner erforderlich, dass die Größe des freien Speicherplatzes auf der Partition, in der sich der Ordner "/var/opt/kaspersky/klnagent_srv/" befindet, den Gesamtumfang der Programmpakete der zu installierenden Anwendungen um ein Vielfaches übertrifft.

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.

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.

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.

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.

Anpassen der Einstellungen der Installer

Dieser Abschnitt enthält Informationen über die Dateien der Installer von Kaspersky Security Center Linux und die Installationseinstellungen, sowie Empfehlung zur Installation des Administrationsservers und des Administrationsagenten im Silent-Modus.

Allgemeine Informationen

Die Installer von Kaspersky Security Center Linux für Windows-Geräte basieren auf der Technologie der Windows Installer. Der Kern des Installers ist das MSI-Paket. Dieses Verpackungsformat der Distribution erlaubt, alle Vorteile der Windows Installer-Technologie zu verwenden: die Skalierbarkeit, die Möglichkeit von System-Patches, das System der Transformation, die Möglichkeit einer zentralisierten Installation von Drittherstellerlösungen, die Transparenz der Anmeldung im Betriebssystem.

Installation im Silent-Modus (mit Antwortdatei)

Das Installationsprogramm des Administrationsagenten besitzt die Möglichkeit zur Verwendung der Antwortdatei (ss_install.xml), in der die Parameter für die Installation im Silent-Modus ohne Benutzerinteraktion gespeichert sind. Die Datei ss_install.xml befindet sich im selben Ordner wie das msi-Paket und wird automatisch bei der Installation im Silent-Modus verwendet. Sie können die Installation im Silent-Modus mit dem Befehlszeilenparameter "/ s" aktivieren.

Beispiel für den Start:

```
setup.exe /s
```

Lesen Sie den Endbenutzer-Lizenzvertrag (EULA), bevor Sie das Installationsprogramm im Silent-Modus starten. 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.

Die Datei "ss_install.xml" stellt eine Instanz des internen Formats für die Parameter des Installers von Kaspersky Security Center Linux dar. Im Lieferumfang der Programmpakete wird die Datei "ss_install.xml" mit den Standardparametern geliefert.

Die Datei ss_install.xml darf nicht manuell geändert werden. Diese Datei wird mithilfe von Kaspersky Security Center Linux bei der Änderung der Parameter der Installationspakete in der Kaspersky Security Center Web Console geändert.

Teilweises Anpassen der Installationseinstellungen durch setup.exe

Beim Start der Programminstallation mittels setup.exe können die Werte beliebiger MSI-Eigenschaften ins msi-Paket übergeben werden.

Der Befehl sieht folgendermaßen aus:

Beispiel:
`/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"`

Installationseinstellungen für den Administrationsserver

Die folgende Tabelle beschreibt die Eigenschaften, die Sie konfigurieren können, wenn Sie Kaspersky Security Center Linux im Silent-Modus installieren.

Einstellungen für die Installation des Administrationsservers im Silent-Modus

Name der Variablen	Notwendig	Beschreibung	Mögliche V
`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 ode 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 KLOAPI-Portnummer des Administrationsservers. Optional. Standardwert ist 13299.	Portnummer
`KLSRV_UNATT_PORT_GUI`	Nein	Die Portnummer für die Benutzeroberfläche des Administrationsservers. Optional. Standardwert ist 13291.	Portnummer
`KLSRV_UNATT_NETRANGETYPE`	Nein	Die ungefähre Anzahl an Geräten, die Sie verwalten möchten: Optional. Standardwert ist 1.	`1` für 1 bis 100 v Geräte. `2` für 101 bis 1.0 vernetzte Gerä `3` für mehr als 1 vernetzte Gerä
`KLSRV_UNATT_DBMS_TYPE`	Ja	Der Typ des Datenbankverwaltungssystems:	`mysql` oder `postgres`

		MySQL (MariaDB) oder Postgres.	
KLSRV_UNATT_DBMS_INSTANCE	Ja	Die IP-Adresse des Datenbankservers.	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.	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_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 des Administrationsservers als Kaspersky Security Center Linux Failover-Cluster, muss die Antwortdatei die folgenden zusätzlichen Variablen enthalten:			
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.	VirtualAdapt oder ExternalLoac
Falls die Variable KLFOC_UNATT_CONN_MODE den Wert VirtualAdapter besitzt, muss die Antwortdatei die fol 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

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 habe die Bedingungen des Endbenutzer-Lizenzvertrags vollständig gelesen, und verstehe und akzeptiere sie. • 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	Zahlenwert.

	sicheren Verbindung mit dem Administrationsserver über das SSL-Protokoll	
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? Aus Kompatibilitätsgründen wird es nicht empfohlen, die Einstellungen der Proxy-Verbindung in den Einstellungen des Installationspakets für den Administrationsagenten festzulegen.	• 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
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	Soll nach der Installation der Dienst des Administrationsagenten gestartet werden? 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.

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 Datenbank des Administrationsservers hinzugefügt. Nach dem Deaktivieren der virtuellen Maschine muss der sie betreffende Eintrag auch aus der Datenbank des Administrationsservers 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.

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.

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.

Für Kaspersky Security Center Linux sind nur jene Szenarien kritisch, bei denen Software von Drittherstellern auf den Geräten mit installiertem Administrationsagenten den Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ betrifft. 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.

Falls irgendwie möglich, muss ein Rollback des Ordners %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ auf den Geräten mit installiertem Administrationsagenten vermieden werden, da eine nochmalige 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 Standard-Tools "klbackup" aus der Backup-Kopie wiederhergestellt werden.

Lokale Installation von Programmen

In diesem Abschnitt wird der Installationsvorgang der Programme beschrieben, die nur lokal auf den Geräten installiert werden können.

Um eine lokale Installation von Programmen auf einem ausgewählten Client-Gerät durchzuführen, müssen Sie über Administratorrechte auf diesem Gerät verfügen.

Gehen Sie wie folgt vor, um Programme auf einem ausgewählten Client-Gerät lokal zu installieren:

1. Installieren Sie auf dem Client-Gerät den Administrationsagenten, und passen Sie die Verbindung des Client-Geräts mit dem Administrationsserver an.

2. Installieren Sie die erforderlichen Programme auf dem Gerät. Folgen Sie dabei den Anweisungen in den Handbüchern zu diesen Programmen.

3. Installieren Sie auf dem Administrator-Arbeitsplatz das Verwaltungs-Plug-in für jedes installierte Programm.

Außerdem unterstützt Kaspersky Security Center Linux die Möglichkeit zur lokalen Installation von Programmen mithilfe eines autonomen Installationspakets. Die Installation aller Programme von Kaspersky wird von Kaspersky Security Center Linux nicht unterstützt.

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 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.

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 Betriebssystem mit 32-Bit:

     ```
     # yum -i klnagent-<Build-Nummer>.i386.rpm
     ```

   - So installieren Sie den Administrationsagenten aus einem RPM-Paket auf einem Betriebssystem mit 64-Bit:

```
# yum -i klnagent64-<Build-Nummer>.x86_64.rpm
```

- So installieren Sie den Administrationsagenten aus einem RPM-Paket auf einem Betriebssystem mit 64-Bit für die Arm-Architektur:

  ```
  # yum -i klnagent64-<Build-Nummer>.aarch64.rpm
  ```

- So installieren Sie den Administrationsagenten aus einem DEB-Paket auf einem Betriebssystem mit 32-Bit:

  ```
  # apt install ./klnagent_<Build-Nummer>_i386.deb
  ```

- So installieren Sie den Administrationsagenten aus einem DEB-Paket auf einem Betriebssystem mit 64-Bit:

  ```
  # apt install ./klnagent64_<Build-Nummer>_amd64.deb
  ```

- So installieren Sie den Administrationsagenten aus einem DEB-Paket auf einem Betriebssystem mit 64-Bit für die Arm-Architektur:

  ```
  # apt install ./klnagent64_<Build-Nummer>_arm64.deb
  ```

2. Führen Sie die Konfiguration des Administrationsagenten aus:

   ```
   # /opt/kaspersky/klnagent64/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 Bestimmungen der EULA zustimmen.
   - Geben Sie `r` ein, um die EULA erneut anzuzeigen.

4. Geben Sie den DNS-Namen oder die statische 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 den Import der Aufgabe 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.

   - 0 – Verbindungs-Gateway nicht verwenden

     Ihr Gerät stellt keine Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway her.

   - Verbindung mit dem Administrationsserver über ein Verbindungs-Gateway herstellen

     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.

Installation des Administrationsagenten im Silent-Modus

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.

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 <Parameter>
   ```

   Dabei steht `Parameter` für eine Liste mit Einstellungen und deren Werten, die durch Leerzeichen getrennt werden (`PARAM1=WERT1 PARAM2=WERT2`).

   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 11 und höher, 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.

Programme im Silent-Modus installieren

Um ein Programm im nicht Silent-Modus zu installieren, gehen Sie wie folgt vor:

1. Öffnen Sie das Programmhauptfenster von Kaspersky Security Center.
2. Wählen Sie in der Konsolenstruktur im Ordner **Remote-Installation** im Unterordner **Installationspakete** das Installationspaket für das betreffende Programm aus oder erstellen Sie ein neues Installationspaket für dieses Programm.

   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 Weisen:

   - 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 Programmen von Kaspersky 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.

Programme mithilfe autonomer Installationspakete installieren

Kaspersky Security Center ermöglicht das Erstellen von autonomen Installationspaketen für Programme. Bei einem autonomen Installationspaket handelt es sich um eine ausführbare Datei, die auf einem Webserver gestellt, per E-Mail verschickt oder auf andere Weise auf ein Client-Gerät übermittelt werden kann. Die empfangene Datei kann lokal auf dem Client-Gerät gestartet werden, um das Programm ohne Beteiligung von Kaspersky Security Center zu installieren.

Um ein Programm mithilfe des autonomen Installationspakets zu installieren, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum gewünschten Administrationsserver her.
2. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.
3. Wählen Sie im Arbeitsbereich das Installationspaket für das gewünschte Programm aus.
4. Starten Sie den Vorgang zum Erstellen eines autonomen Installationspakets auf eine der folgenden Weisen:
   - Klicken Sie mit der rechten Maustaste auf das Installationspaket und wählen Sie **Autonomes Installationspaket erstellen** aus.
   - Klicken Sie mit der rechten Maustaste in den Arbeitsbereich des Installationspaketes und wählen Sie **Autonomes Installationspaket erstellen** aus.

   Daraufhin wird der Assistent für das Erstellen eines autonomen Installationspakets gestartet. Folgen Sie den Anweisungen des Assistenten.

   Wählen Sie im letzten Schritt des Assistenten eine Methode für die Übertragung des autonomen Installationspakets auf das Client-Gerät aus.
5. Übertragen Sie das autonome Installationspaket für das Programm auf das Client-Gerät.
6. 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.

Einstellungen des Installationspakets des Administrationsagenten

Um die Einstellungen des Installationspakets des Administrationsagenten anzupassen, gehen Sie wie folgt vor:

1. Wählen Sie im Ordner **Remote-Installation** der Konsolenstruktur den Unterordner **Installationspakete** aus.

   Der Ordner **Remote-Installation** ist standardmäßig ein Unterordner des Ordners **Erweitert**.
2. Klicken Sie mit der rechten Maustaste auf das Installationspaket des Administrationsagenten und wählen Sie **Eigenschaften** aus.

Daraufhin wird das Eigenschaftenfenster des Installationspakets des Administrationsagenten geöffnet.

Allgemein

Der Abschnitt **Allgemein** enthält allgemeine Informationen zum Installationspaket:

- 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

Einstellungen

In diesem Abschnitt können Sie Einstellungen anpassen, die für die Funktionstüchtigkeit des Administrationsagenten sofort nach dessen Installation erforderlich sind. Die Einstellungen in diesem Abschnitt sind nur auf Geräten verfügbar, die unter Windows laufen.

In der Einstellungsgruppe **Zielordner** können Sie einen Ordner auf dem Client-Gerät auswählen, in dem der Administrationsagent installiert werden soll.

- **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.

In der Einstellungsgruppe weiter unten können Sie ein Kennwort für die Remote-Deinstallation des Administrationsagenten angeben:

- **Deinstallationskennwort verwenden**

  Wenn die Option aktiviert ist, können Sie nach einem Klick auf **Ändern** das Kennwort für die Deinstallation des Programms angeben (nur für Administrationsagenten auf Geräten unter einem Windows-Betriebssystem verfügbar).

  Diese Option ist standardmäßig deaktiviert.

- **Status**

  Status des Kennworts: **Kennwort gesetzt** oder **Kennwort nicht gesetzt**.

  Standardmäßig ist kein Kennwort gesetzt.

- **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, Exchange-Server für mobile Geräte 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.

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:

- **Administrationsserver**

  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 **Durchsuchen** angegeben werden kann.

Wenn diese Option deaktiviert ist, wird die Zertifikatsdatei bei der ersten Verbindung des Administrationsagenten über die Adresse, die im Feld **Serveradresse** 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.

Dieses Kontrollkästchen ist standardmäßig ausgewählt.

- **SSL 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.

- **Ports des Administrationsagenten in der Windows-Firewall öffnen**

  Wenn diese Option aktiviert ist, werden die vom Administrationsagenten verwendeten UDP-Ports zur Liste der Ausschlüsse der Microsoft Windows Firewall hinzugefügt.

  Diese Option ist standardmäßig aktiviert.

- **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, 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.

Aus Kompatibilitätsgründen wird es nicht empfohlen, die Einstellungen der Proxy-Verbindung in den Einstellungen des Installationspakets für den Administrationsagenten festzulegen.

Erweitert

Im Abschnitt **Erweitert** können Sie konfigurieren, wie das Verbindungs-Gateway verwendet wird. Zu diesem Zweck können Sie Folgendes tun:

- Verwenden Sie den Administrationsagenten als Verbindungsgateway in der demilitarisierten Zone (DMZ), um sich mit dem Administrationsserver zu verbinden, mit ihm zu kommunizieren und während der Datenübertragung die Daten auf dem Administrationsagenten sicher aufzubewahren.
- Verbinden Sie sich unter Verwendung eines Verbindungsgateways mit dem Administrationsserver, um die Anzahl der Verbindungen zum Administrationsserver zu reduzieren. Geben Sie in diesem Fall im Feld **Verbindungs-Gateway-Adresse** die Adresse des Geräts ein, das als Verbindungs-Gateway fungieren soll.
- Konfigurieren Sie die Verbindung für die Virtual Desktop Infrastructure (VDI), wenn Ihr Netzwerk virtuelle Maschinen enthält. Gehen Sie dafür wie folgt vor:
  - **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 VDI 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.

Zusätzliche Komponenten

In diesem Abschnitt können Sie weitere Komponenten für die gemeinsame Installation mit dem Administrationsagenten auswählen.

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.

Revisionsverlauf

In diesem Abschnitt 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.

Einstellungen für das Installationspaket des Administrationsagenten, die für ein spezifisches Betriebssystem verfügbar sind, werden in der folgenden Tabelle aufgelistet.

Einstellungen des Installationspakets des Administrationsagenten

Abschnitt der Eigenschaft	Windows	Mac	Linux
Allgemein	✓	✓	✓
Einstellungen	✓	–	–
Verbindung	✓	✓ (mit Ausnahme der Optionen **Ports des Administrationsagenten in der Windows-Firewall öffnen** und **Nur automatische Erkennung des Proxyservers verwenden**)	✓ (mit Ausnahme der Optionen **Ports des Administrationsagenten in der Windows-Firewall öffnen** und **Nur automatische Erkennung des Proxyservers verwenden**)
Erweitert	✓	✓	✓
Zusätzliche Komponenten	✓	✓	✓
Tags	✓	✓ (mit Ausnahme der Regeln zur automatischen Zuweisung von Tags)	✓ (mit Ausnahme der Regeln zur automatischen Zuweisung von Tags)
Revisionsverlauf	✓	✓	✓

Kaspersky Security Center Linux Webserver

Der Kaspersky Security Center Linux Webserver (Im Weiteren der 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 jede Weise an den Benutzer übermitteln, wie etwa per E-Mail.

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

Webserver-Einstellungen

Wenn Sie den Webserver noch weiter anpassen möchten, können Sie in den Eigenschaften des Webservers die Ports für die Protokolle HTTP (8060) und HTTPS (8061) wechseln. Ferner ist neben dem Wechsel der Ports der Wechsel des Serverzertifikats für das HTTPS-Protokoll und der Wechsel des FQDN-Namens des Webservers für das HTTP-Protokoll möglich.

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.

Client-Geräte verwalten

Dieser Abschnitt beschreibt die Verwaltung von Geräten in den Administrationsgruppen.

Einstellungen eines verwalteten Geräts

Um die Einstellungen eines verwalteten Geräts anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete 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.

Im oberen Teil des Eigenschaftenfensters werden als Hauptgruppen der Einstellungen die folgenden Registerkarten 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 lässt sich der Name des Client-Geräts in der Administrationsgruppe anzeigen und ändern.

  - **Beschreibung**

    In diesem Feld können Sie eine zusätzliche Beschreibung für das Client-Gerät eingeben.

  - **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.

  - **Gerätebesitzer**

    Name des Gerätebesitzers. Sie können einen Benutzer als Gerätebesitzer zuweisen oder entfernen, indem Sie auf den Link **Gerätebesitzer verwalten** klicken.

  - **Vollständiger Gruppenname**

    Administrationsgruppe, zu der das Client-Gerät gehört.

  - **Letzte Aktualisierung der Antiviren-Datenbanken**

    Datum des letzten Updates der Antiviren-Datenbanken oder der Programme 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 der Geräte-Erstellung innerhalb von Kaspersky Security Center Linux.

- 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.

- Im Abschnitt **Netzwerk** werden folgende Informationen zu den Netzwerkeinstellungen des Client-Geräts angezeigt:

  - 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-Gerätes.

  - **IPv6-Adresse**

- Im Abschnitt **System** werden Daten zum Betriebssystem, das auf dem Client-Gerät installiert ist, angezeigt:

  - **Betriebssystem**
  - **CPU-Architektur**
  - **Gerätename**
  - Typ der virtuellen Maschine

Erzeuger 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.

- Im Abschnitt **Schutz** werden die folgenden Informationen über den Status des Antiviren-Schutzes auf dem Client-Gerät angezeigt:

  - **Sichtbar**

    Sichtbarkeitsstatus der Datenverschlüsselung 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**

    Für Status des Schutzes für das Client-Gerät und der Verbindung zum Administrationsserver.

  - **Schutzstatus**

    Dieses Feld zeigt den aktuellen Status des Echtzeitschutzes auf dem Client-Gerät an.

    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 einem Client-Gerät gefundenen Bedrohungen seit der Installation des Antiviren-Programms (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 für mobile Geräte 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.

- Im Abschnitt **Gerätestatus wird vom Programm bestimmt** werden Daten über den Gerätestatus, der durch das auf dem Gerät installierte verwaltete Programm bestimmt wird, angezeigt. Der Gerätestatus kann von dem durch Kaspersky Security Center Linux vorgegebenen Status abweichen.

- **Programme**

  Diese Registerkarte listet alle Kaspersky-Programme auf, die auf dem Client-Gerät installiert sind. Sie können den Programmnamen anklicken, um sich allgemeine Informationen über das Programm, eine Liste mit allen auf dem Gerät aufgetretenen Ereignissen und die Programmeinstellungen anzeigen zu lassen.

- **Aktive Richtlinien und Richtlinienprofile**

  Diese Registerkarte listet die Richtlinien und Richtlinienprofile auf, die derzeit auf dem verwalteten Gerät aktiven sind.

- **Aufgaben**

  In 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. Sollte keine Verbindung hergestellt sein, erscheint der Status nicht.

- **Ereignisse**

  In der Registerkarte **Ereignisse** werden Ereignisse angezeigt, die für das ausgewählte Client-Gerät auf dem Administrationsserver registriert wurden.

- **Sicherheitsprobleme**

In 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 Verwaltungsprogrammen von Kaspersky als auch manuell durch den Administrator erstellt werden. Wenn beispielsweise einige Benutzer immer wieder Schadsoftware von ihrem Wechseldatenträger auf das Gerät 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 für 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 die Änderung des Status eines Geräts auf *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 dem Kaspersky-Programm bestimmt, dass das den Vorfall erstellt hat. Bearbeitete Sicherheitsvorfälle können in der Liste durch Aktivieren des Kontrollkästchens in der Spalte **Bearbeitet** gekennzeichnet werden.

- **Tags**

  In 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 Programme und der Programm-Updates anzeigen lassen und die Darstellung der Programm-Registry konfigurieren.

  Die Daten über die installierten Programme sind verfügbar, wenn der auf dem Client-Gerät installierte Administrationsagent die erforderlichen Daten auf den Administrationsserver überträgt. Die Einstellungen für die Übertragung der Informationen auf den Administrationsserver können Sie im Eigenschaftenfenster des Administrationsagenten oder seiner Richtlinie im Abschnitt **Datenverwaltung** anpassen.

  Durch Klicken auf einen Programmnamen wird ein Fenster geöffnet, das die Anwendungsdetails und eine Liste der für die Anwendung installierten Update-Pakete enthält.

- **Ausführbare Dateien**. In diesem Abschnitt werden ausführbare Dateien angezeigt, die auf dem Client-Gerät entdeckt wurden.

- **Verteilungspunkte**. In diesem Abschnitt finden Sie 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 das Programm 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**. In diesem Abschnitt finden Sie Informationen zur Hardware, die auf dem Client-Gerät installiert ist.

- **Verfügbare Updates**. In diesem Abschnitt können Sie sich die Liste der auf dem Gerät gefundenen Software-Updates anzeigen lassen, die nicht installiert wurden.

- **Schwachstellen in Programmen**. Dieser Abschnitt bietet Informationen über die Schwachstellen von Drittanbietersoftware, die auf den Client-Geräten installiert ist.

  Um die Schwachstellen in einer Datei zu speichern, aktivieren Sie die Kontrollkästchen neben den Schwachstellen, die Sie speichern möchten, 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 im Abschnitt Schwachstellen angezeigt, die durch einen Patch geschlossen werden können.

    Ist diese Option deaktiviert, werden im Abschnitt Schwachstellen angezeigt, die durch einen Patch geschlossen werden können, sowie Schwachstellen, für die kein Patch vorhanden ist.

    Diese Option ist standardmäßig aktiviert.

  - Schwachstellen-Eigenschaften

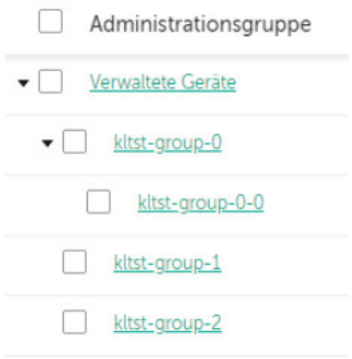
Wählen Sie in der Liste eine Software-Schwachstelle aus, um die Eigenschaften der ausgewählten Software-Schwachstelle in einem separaten Fenster anzuzeigen. In dem Fenster können Sie Folgendes tun:

- Schwachstellen in Programmen auf diesem verwalteten Gerät ignorieren (in der Verwaltungskonsole oder in der Kaspersky Security Center Web Console).
- Liste mit Korrekturen anzeigen, die für die Schwachstelle empfohlen werden.
- Software-Updates manuell angeben, um eine Schwachstelle zu beheben (in der Verwaltungskonsole oder 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.

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 **Assets (Geräte)** → **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 **Assets (Geräte)** → **Gruppenhierarchie**.
2. Klicken Sie auf die Schaltfläche **Importieren**.

Daraufhin wird der Assistent für das Erstellen einer Administrationsgruppenstruktur gestartet. Folgen Sie den Anweisungen des Assistenten.

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 **Assets (Geräte)** → **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 eines Programms* 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, die Zuweisung von Administrationsagenten entsprechend dem Standardszenario und so weiter.

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. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verschiebungsregeln**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.
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.

- **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. Um die Priorität einer Verschiebungsregel zu erhöhen oder zu verringern, verschieben Sie die Regel mit der Maus in der Liste nach oben bzw. nach unten.

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 **Assets (Geräte)** → **Verschiebungsregeln**.

   - Wechseln 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.

   - **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 Programme, 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:

- **Auf Geräte ohne angegebene Tags anwenden**

  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:

- **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.

- 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.

- Von einem anderen Administrationsserver verwaltet

  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 Programme

Auf dieser Registerkarte können Sie eine Regel zum Verschieben von Geräten basierend auf den verwalteten Programmen 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.

- **Programme**

Geben Sie an, welche verwalteten Programme auf Client-Gerät installiert sein müssen, damit für diese Geräte eine Verschiebungsregel gilt. Sie können beispielsweise **Kaspersky Security Center 15 Administrationsagent** oder **Kaspersky Security Center 15 Administrationsserver** angeben.

Wenn Sie keine verwaltetes Programm auswählen, trifft die Bedingung nicht zu.

- Version des Betriebssystems

  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.

- Bitzahl des Betriebssystems

  Sie können Client-Geräte anhand der Bitanzahl des Betriebssystems auswählen. Im Block **Bitzahl des Betriebssystems** können Sie einen der folgenden Werte auswählen:

  - **Unbekannt**
  - **x86**
  - **AMD64**
  - **IA64**

  So überprüfen Sie die Bitanzahl des Betriebssystems der Client-Geräte:

  1. Wechseln Sie im Hauptmenü zum Abschnitt **Assets (Geräte)** → **Verwaltete Geräte**.
  2. Klicken Sie auf die Schaltfläche **Spalteneinstellungen** ( ) auf der rechten Seite.
  3. Aktivieren Sie die Option **Bitzahl des Betriebssystems** und klicken Sie anschließend auf die Schaltfläche **Speichern**.

     Danach wird die Bitanzahl des Betriebssystems für jedes verwaltete Gerät angezeigt.

- Service Pack-Version des Betriebssystems

  In diesem Feld können Sie die Version des Updatepakets für das Betriebssystem angeben (im Format *X.Y*), das vorhanden sein muss, damit auf dem Gerät die Regel für das Verschieben angewandt 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.

- Build-Version des Betriebssystems

  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.

- Releasenummer des Betriebssystems

  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 Domänensicherheitsgruppe**

  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. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.
2. Klicken Sie auf den Link **Aktueller Pfad:** `<aktueller Pfad>` über der Liste.
3. Wählen Sie im nächsten Fenster die Administrationsgruppe aus, zu der Sie die Geräte hinzufügen möchten.
4. Klicken Sie auf die Schaltfläche **Geräte hinzufügen**.

   Daraufhin wird der Assistent zum Verschieben von Geräten gestartet.
5. 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 Datenbank des Administrationsservers 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.
  - 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: , \ / * ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

6. Zeigen Sie die Liste der Geräte an, die der Administrationsgruppe hinzugefügt werden sollen. Sie können die Liste bearbeiten, indem Sie Geräte hinzufügen oder entfernen.
7. 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, gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**, klicken Sie auf den Pfad-Link im Feld **Aktueller Pfad** und wählen Sie im sich öffnenden linken Bereich eine Administrationsgruppe aus.

- Um die Gruppe **Nicht zugeordnete Geräte** im Hauptmenü zu öffnen, wechseln Sie zu **Gerätesuche und Bereitstellung** → **Nicht zugeordnete Geräte**.

2. Wenn die Administrationsgruppe Cluster oder Server-Arrays enthält, wird der Abschnitt **Verwaltete 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 **Verwaltete 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. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete 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-Programm

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.

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:

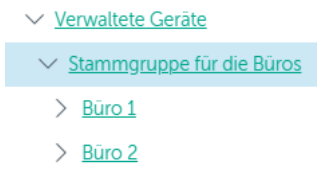
- Aufbau der Struktur der Administrationsgruppen unter Berücksichtigung der Netztopologie. Die Struktur der Administrationsgruppen muss die Netztopologie nicht unbedingt genau widerspiegeln. Es ist ausreichend, wenn den einzelnen Teilen des Netzwerkes bestimmte Administrationsgruppen entsprechen. Die 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.

Um Verteilungspunkte automatisch zuzuweisen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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 manuell bestimmen, nachdem Sie deren Anzahl und Konfiguration berechnet haben.

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

Um ein Gerät manuell zum Verteilungspunkt zu bestimmen, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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.

     - **Multicast verwenden**

       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 eines Programms aus einem Installationspaket in eine Gruppe von Client-Geräten. Dagegen reduziert es die Installationsdauer, wenn Sie ein Programm 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 IPv4-Adresse, über die Remote-Geräte eine Verbindung zum Verteilungspunkt herstellen.

- **Updates verteilen**

  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.

- **Installationspakete verteilen**

  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.

- **Push-Server ausführen**

  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 **Aufgaben 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.

- Im Unterabschnitt **Internetverbindungseinstellungen** können Sie die Einstellungen für den Internetzugang 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 das Programm 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 für 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 über 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.

- **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. 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. 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.

- Konfigurieren Sie die Abfrage des Domänencontrollers mittels eines Verteilungspunkts.

  - **Abfrage des Domänencontrollers**

    Sie können für Domänencontroller die Gerätesuche aktivieren.

    Wenn Sie die Option **Abfrage des Domänencontrollers aktivieren** auswählen, können Sie Domänencontroller für die Abfrage auswählen und deren Abfragezeitplan 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.

    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-browser" 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.

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 **Assets (Geräte)** → **Verwaltete Geräte**.
2. Klicken Sie im Feld **Aktueller Pfad** über der Liste der verwalteten Geräte auf den Pfad-Link.
3. Wählen Sie im geöffneten linken Bereich eine Administrationsgruppe aus, für welche Sie die zugewiesenen Verteilungspunkte ansehen möchten.

   Dadurch wird der Menüpunkt **Verteilungspunkte** aktiviert.
4. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verteilungspunkte**.
5. Um der Administrationsgruppe neue Verteilungspunkte hinzuzufügen, klicken Sie auf die Schaltfläche **Zuweisen**.
6. 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 ein verwaltetes Programm 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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 **Push-Server ausführen**.

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.

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 in bestimmten Fällen das Sichtbarkeits-Flag des Gerätes im Netzwerk berücksichtigt (siehe folgende Tabelle). 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
Es wurde keine Sicherheitsanwendung 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 Datenbank des Administrationsservers 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 Datenbank des Administrationsservers 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 werden erkannt	Die Anzahl der unbearbeiteten Objekte im Ordner **Aktive Bedrohungen** übersteigt den angegebenen Wert.	Über 0 Elemente.
Neustart erforderlich	Das Gerät ist im Netzwerk sichtbar, aber ein Programm erfordert aufgrund einer der	Über 0 Minuten.

	angegeben Bedingungen einen Neustart des Gerätes, der nicht innerhalb des festgelegten Zeitraums ausgeführt wurde.	
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 Programme 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.
Die letzte Suche nach Windows-Updates liegt lange zurück	Das Gerät ist im Netzwerk sichtbar, aber die Aufgabe *Windows-Updates synchronisieren* 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 Verwaltungsprogrammen von Kaspersky als auch manuell durch den Administrator erstellt werden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Gerätestatus wird vom Programm bestimmt	Der Gerätestatus wird vom verwalteten Programm bestimmt.	• Umschalter deaktiviert. • Umschalter 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 Kaspersky Security Center Linux von der vorhergehenden Version upgraden, bleiben die Werte für die Zuweisung der Statusvarianten *Kritisch* oder *Warnung* für die Bedingung **Die Datenbanken sind veraltet** unverändert.

Wenn Kaspersky Security Center Linux einem Gerät einen Status zuweist, wird für bestimmte Bedingungen (siehe Spalte "Beschreibung der Bedingung" in der obigen Tabelle) das Sichtbarkeits-Flag berücksichtigt. 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*.

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. Öffnen Sie das Eigenschaftenfenster auf eine der folgenden Weisen:
   - Wählen Sie im Ordner **Richtlinien** im Kontextmenü der Richtlinie eines Administrationsservers **Eigenschaften** aus.
   - Wählen Sie im Kontextmenü einer Administrationsgruppe den Punkt **Eigenschaften** aus.
2. Wählen Sie im nächsten Fenster **Eigenschaften** im Bereich **Abschnitte** den Punkt **Gerätestatus** aus.
3. Aktivieren Sie im rechten Bereich im Abschnitt **Werte mit Status "Kritisch"** das Kontrollkästchen neben einer Bedingung in der Liste.

   Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

4. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.

   Sie können Werte für bestimmte Bedingungen festlegen, aber nicht für alle.

5. 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. Öffnen Sie das Eigenschaftenfenster auf eine der folgenden Weisen:
   - Wählen Sie im Ordner **Richtlinien** im Kontextmenü der Richtlinie des Administrationsservers den Punkt **Eigenschaften** aus.
   - Wählen Sie im Kontextmenü der Administrationsgruppe den Punkt **Eigenschaften** aus.
2. Wählen Sie im nächsten Fenster **Eigenschaften** im Bereich **Abschnitte** den Punkt **Gerätestatus** aus.
3. Aktivieren Sie im rechten Bereich im Abschnitt **Werte mit Status "Warnung"** das Kontrollkästchen neben einer Bedingung in der Liste.

Sie können nur die Einstellungen ändern, die in der übergeordneten Richtlinie nicht gesperrt sind.

4. Legen Sie den erforderlichen Wert für die ausgewählte Bedingung fest.

   Sie können Werte für bestimmte Bedingungen festlegen, aber nicht für alle.

5. 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 werden erkannt**). Vordefinierte Auswahlen können nicht gelöscht werden. Sie können auch zusätzliche *benutzerdefinierte Auswahlen* definieren und anpassen.

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. Wechseln Sie im Hauptmenü zum Abschnitt **Assets (Geräte)** → **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 Filtersymbol ( ), 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. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **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 miteinbeziehen** 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 **Assets (Geräte)** → **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

Ist die Option aktiviert, so wird die vorgegebene Auswahlbedingung umgekehrt. Alle Geräte, die diese Bedingung nicht erfüllen, werden in die Auswahl aufgenommen.

Diese Option ist standardmäßig deaktiviert.

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.

- Von einem anderen Administrationsserver verwaltet

  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:

- Das Gerät befindet sich in einer Organisationseinheit der Domäne

  Wenn diese Option aktiviert ist, werden in die Auswahl Geräte aus der Domänenorganisationseinheit aufgenommen, die im Eingabefeld angegeben wurde.

  Diese Option ist standardmäßig deaktiviert.

- Das Gerät ist Mitglied der Domänensicherheitsgruppe

  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.

- Wechsel des Verbindungsprofils

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**. Das Programm 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 des verwalteten Programms 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 Programme** können Sie Kriterien für die Aufnahme von Geräten in eine Auswahl anhand der Status der Komponenten der verwalteten Programme 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 Programmen** können Sie die Kriterien für die Aufnahme von Geräten in die Auswahl anhand der Liste von möglichen von einem verwalteten Programm 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 Programme aufgelistet ist, haben Sie die Möglichkeit, dieses Problem in allen Listen automatisch auszuwählen.

Sie können die Kontrollkästchen für die Beschreibung der Status der verwalteten Programme aktivieren, bei deren Empfang die Geräte in die Auswahl aufgenommen werden. Wenn Sie einen Status auswählen, der für mehrere Programme 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 Version des Updatepakets für das Betriebssystem angeben (im Format *X.Y*), das vorhanden sein muss, damit auf dem Gerät die Regel für das Verschieben angewandt wird. Standardmäßig ist keine Version angegeben.

- Bitzahl 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-Version 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.

- Releasenummer 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.

- **RAM-Größe in 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.

- **Speichergröße 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 Programmen anpassen:

- **Programmname**

  In dieser Dropdown-Liste können Sie ein Programm auswählen. Die Geräte, auf denen dieses Programm installiert ist, werden in die Auswahl aufgenommen.

- **Programmversion**

  Geben Sie in diesem Eingabefeld die Version des ausgewählten Programms ein.

- **Hersteller**

In dieser Dropdown-Liste können Sie den Hersteller des auf dem Gerät installierten Programms auswählen.

- **Programmstatus**

  Dropdown-Liste, in der Sie den Status des Programms auswählen können (*Installiert*, *Nicht installiert*). Die Geräte, auf denen das angegebene Programm 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 Programme. Nachdem Sie das Kontrollkästchen aktiviert haben, ändern sich die Felder **Programmname**, **Programmversion** und **Programm-Status** in **Update-Name**, **Update-Version** und **Status**.

  Diese Option ist standardmäßig deaktiviert.

- **Name der inkompatiblen Sicherheitsanwendung**

  In dieser Dropdown-Liste können Sie Sicherheitsanwendungen von Drittherstellern auswählen. Bei der Suche werden Geräte in die Auswahl aufgenommen, auf denen das ausgewählte Programm installiert wurde.

- **Programm-Tag**

  In dieser Dropdown-Liste können Sie einen Programm-Tag auswählen. Alle Geräte, auf denen Programme installiert sind, die den ausgewählten Tag in der Beschreibung haben, werden in die Geräteauswahl aufgenommen.

- **Auf Geräte ohne angegebene Tags anwenden**

  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 Programmen von Kaspersky

Im Unterabschnitt **Programme von Kaspersky** können Sie die Kriterien für die Aufnahme von Geräten anhand des ausgewählten verwalteten Programms konfigurieren:

- **Programmname**

  In der Dropdown-Liste können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl wählen, wenn die Suche anhand des Namens des Kaspersky-Programms erfolgt.

  In der Liste sind nur die Programme aufgeführt, für die Verwaltungs-Plug-ins im Administrator-Arbeitsplatz installiert sind.

  Wurde kein Programm gewählt, wird kein Kriterium angewandt.

- **Programmversion**

  In diesem Eingabefeld können Sie ein Kriterium für die Aufnahme von Geräten in die Auswahl angeben, wenn die Suche nach Versionsnummer des Kaspersky-Programms 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 Programmnamen oder der Update-Paketnummer erfolgt.

  Ist dieses Feld leer, wird kein Kriterium angewandt.

- **Programm-Status**

  Dropdown-Liste, in der Sie den Status des Programms auswählen können (*Installiert*, *Nicht installiert*). Die Geräte, auf denen das angegebene Programm 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 Programm-Module 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**. Das Programm 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**. Das Programm 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 Programmen, 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 Programmen versendet. Diese Option zeigt, dass die Programme 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.

- Muss vorhanden sein

  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.

- Darf nicht vorhanden sein

  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. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **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

Dieser Abschnitt beschreibt Geräte-Tags und enthält eine Anleitung für deren Erstellung und Änderung sowie für die manuelle bzw. automatische Zuweisung von Tags an Geräte.

Über 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-Kennzeichnung wird von Kaspersky Security Center Linux auf eine der folgenden Arten ausgeführt:

- In Übereinstimmung mit den angegebenen Tagging-Regeln.
- Durch eine Anwendung.

> Es wird nicht empfohlen, verschiedene Tag-Methoden zu verwenden, um dasselbe Tag zuzuweisen. Wenn das Tag beispielsweise durch die Regel zugewiesen wird, wird davon abgeraten, dieses Tag manuell Geräten zuzuweisen.

Wenn die Tags durch Regeln zugewiesen wurden, werden Geräte automatisch mit Tags versehen, 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 Programmen 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.

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. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **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 **Assets (Geräte)** → **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.

Um ein Geräte-Tag zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Tags** → **Tags des Geräts**.
   Die Aufgabenliste wird angezeigt.
2. Wählen Sie den Arbeitsbereich 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 Tag-Kennzeichnung 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, jedoch nicht aus der Tag-Liste. 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 einem Programm oder einem Administrationsagenten zugewiesen wurde. Um so Tag von Ihrem Gerät zu entfernen, verwenden Sie das Tool "klscflag".

Geräte mit zugewiesenen Tags anzeigen

So zeigen Sie Geräte an, denen ein Tag zugewiesen ist:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **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 **Verwaltete Geräte** des Hauptmenüs weitergeleitet, wobei die Geräte nach dem Tag gefiltert sind, auf dessen Link zum **Geräte anzeigen**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. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete 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 sehen, wie das Tag zugewiesen wurde.

Sie können dem Gerät ein anderes Tag zuweisen oder ein bereits zugewiesenes Tag entfernen. Darüber hinaus können Sie alle Geräte-Tags ansehen, die auf dem Administrationsserver vorhanden sind.

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 **Assets (Geräte)** → **Verwaltete 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 Programmen oder Administrationsagenten zugewiesen wurden, nicht manuell entfernen. Verwenden Sie zum Entfernen dieser Tags 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 **Assets (Geräte)** → **Tags** → **Regeln für die automatische Tag-Zuweisung**.
- Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **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 umfassen.
   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.

   - **Programme** – Vorhandensein des Administrationsagenten auf dem Gerät, Typ, Version und Betriebssystemarchitektur.
   - **Virtuelle Maschinen** – Das Gerät gehört zu einem speziellen Typ für virtuelle Maschinen.
   - **Programm-Registry** – Vorhandensein von Programmen 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.

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 einem Windows-Betriebssystem die folgenden Verschlüsselungstypen verwalten:

- BitLocker-Laufwerkverschlüsselung
- Kaspersky-Festplattenverschlüsselung

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:

Wechseln 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 eines Programms 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:

Wechseln 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 **Assets (Geräte)** → **Verwaltete Geräte**.
2. Klicken Sie auf den Namen eines verwalteten Geräts.
3. Wechseln 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 Berechtigungen für den Zugriff 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 Programmen auf verschlüsselte Dateien. Dieser Bericht ist hilfreich, wenn nicht autorisierte Benutzer oder Programme versuchen, auf verschlüsselte Dateien oder Laufwerke zuzugreifen.

Im Abschnitt **Überwachung und Berichterstattung** → **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 Berechtigungen für den Zugriff 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. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Verschlüsselung und Datenschutz**.

3. 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.

4. 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 für Windows 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 von Kaspersky Endpoint Security für Windows.

Um Zugriff auf ein sich im autonomen Modus befindliches, verschlüsseltes Laufwerk zu gewähren, gehen Sie wie folgt vor:

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/12.3/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.

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 das Programm **Kaspersky Security Center 15** 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 Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen festlegen oder eine neue erstellen.

Sie können diese Option beispielsweise zum Starten einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die in einer bestimmten Administrationsgruppe enthalten sind.

- **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.

  Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Vielleicht wollen 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 Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen festlegen.

  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.

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. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Gruppenhierarchie**.
2. Klicken Sie auf den Namen der gewünschten Administrationsgruppe.

   Das Eigenschaftenfenster der übergeordneten Administrationsgruppe wird geöffnet.

3. Wechseln 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.

   - **Vererben der Einstellungen für 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.

5. Aktivieren oder deaktivieren Sie im Abschnitt **Geräteaktivität** die folgenden Optionen:

   - **Administrator benachrichtigen, wenn Gerät inaktiv seit mehr als (Tage)**

     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 mehr als (Tage)**

     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.

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 **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf die Schaltfläche **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 **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf die Schaltfläche **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, ausschalten oder neu starten). Geben Sie optional die Meldung der Benutzeraufforderung und die Option **Wartezeit vor dem erzwungenen Schließen von Programmen in gesperrten Sitzungen (Min.)** für die Befehle zum Ausschalten und Neustarten an.

6. Starten Sie die erstellte Aufgabe.

Nach Abschluss der Aufgabe wird der Befehl (Einschalten, Ausschalten oder Neustarten) auf ausgewählten Geräten ausgeführt.

Kaspersky-Programme bereitstellen

Dieser Abschnitt beschreibt die Bereitstellung von Kaspersky-Programmen 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 Programme 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-Programmen erfolgt schrittweise:

1. **Download des Verwaltungs-Web-Plug-ins für das Programm**

   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-Programmen 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 eines Programms 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.

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: Jedes Programm besitzt Richtlinien und Aufgaben und diese Programme 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 Programme erstellt.
- Die Zeitpläne der Aufgaben werden gemäß Ihren Anforderungen angepasst.
- Die ausgewählten Programme wurden auf den ausgewählten Client-Geräten verteilt oder werden nach Zeitplan verteilt.

Verwaltungs-Plug-ins für Kaspersky-Programme hinzufügen

Um ein Kaspersky-Programm 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. Wechseln Sie im Hauptmenü zu **Einstellungen** → **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 für Kaspersky-Programme herunterladen und erstellen

Wenn Ihr Administrationsserver über einen Internetzugang verfügt, können Sie die Installationspakete für Kaspersky-Programme über die Kaspersky-Webserver erstellen.

Um ein Installationspaket für ein Kaspersky-Programm herunterzuladen und zu erstellen:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Installationspakete**.
   - Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** → **Installationspakete**.

   Benachrichtigungen über neue Pakete für Kaspersky-Programme 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.

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 ein Programm von Kaspersky erstellen**.

Eine Liste der Installationspakete, die auf den Kaspersky-Webservern verfügbar sind, wird angezeigt. Die Liste enthält nur Installationspakete von den Programmen, die zu der aktuell genutzten Version von Kaspersky Security Center Linux kompatibel sind.

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.

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.

   Der Download des Installationspakets auf den Administrationsserver beginnt. Sie können das Fenster des Assistenten schließen, oder mit dem nächsten Schritt der Anleitung fortfahren. Wenn sie das Fenster des Assistenten schließen, wird der Download im Hintergrund fortgesetzt.

   Um den Fortschritt des Downloadvorgangs des Installationspakets zu verfolgen:

   a. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Datenverwaltung** → **Installationspakete** → **In Bearbeitung ()**.

   b. Sie können den Fortschritt in den Spalten **Download-Fortschritt** und **Download-Status** der Tabelle verfolgen.

   Wenn der Vorgang abgeschlossen ist, wird das Installationspaket der Liste auf der Registerkarte **Heruntergeladen** hinzugefügt. Wenn der Downloadvorgang anhält und der Downloadstatus zu **EULA akzeptieren** wechselt, klicken Sie auf den Namen des Installationspakets und fahren Sie mit dem nächsten Schritt der Anleitung fort.

   > 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. Bei einigen Programmen von Kaspersky wird während des Downloads die Schaltfläche **EULA anzeigen** angezeigt. Wird diese angezeigt, gehen Sie wie folgt vor:

   a. Klicken Sie auf die Schaltfläche **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.

7. 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.

Installationspakete aus einer Datei erstellen

Mit benutzerdefinierten Installationspaketen können Sie die folgenden Aufgaben ausführen:

- Um ein beliebiges Programm (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 das Programm im Silent-Modus zu installieren.

So erstellen Sie ein benutzerdefiniertes Installationspaket:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.
   - Wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Installationspakete**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

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 aus einer Datei erstellen** aus.

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.

6. Wenn Sie die Datei einer Kaspersky-App angegeben haben, werden Sie möglicherweise aufgefordert, den Endbenutzer-Lizenzvertrag (EULA) für die App 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.

Sie können bestimmte Befehlszeilenparameter angeben, um das Programm im Silent-Modus aus dem Installationspaket zu installieren. Die Angabe von Befehlszeilenparametern ist optional.

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.
  - **Quelle**. Der Programmhersteller.
  - **Programm**. Das im benutzerdefinierten Installationspaket enthaltene Programm.
  - **Version**. Programmversion.
  - **Sprache**. Sprache des Programms, das im benutzerdefinierten Installationspaket enthalten ist.
  - **Größe (MB)**. Größe des Installationspakets.
  - **Betriebssystem**. Typ des Betriebssystems, für welches das Installationspaket vorgesehen ist.
  - **Erstellt**. Erstellungsdatum des Installationspaketes.
  - **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 (Installer.exe). 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 ein Programm zu installieren. Sie können autonome Installationspakete für Programme von Kaspersky und für Drittanbieter-Programme erstellen. Um ein autonomes Installationspaket für ein Drittanbieter-Programm zu erstellen, müssen Sie ein benutzerdefiniertes Installationspaket erstellen.

Stellen Sie sicher, dass unbefugte Personen keinen Zugriff auf das autonome Installationspaket haben.

So erstellen Sie ein autonomes Installationspaket:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.
   - Wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Installationspakete**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

2. Wählen Sie in der Liste der Installationspakete ein Installationspaket aus und klicken Sie oberhalb der Liste auf **Bereitstellen**.

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.

4. Stellen Sie sicher, dass die Option **Administrationsagent gemeinsam mit diesem Programm installieren** aktiviert ist, wenn Sie den Administrationsagenten zusammen mit dem ausgewählten Programm installieren möchten.

   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 das ausgewählte Programm 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 dasselbe Programm erneut erstellen möchten. Das autonome Installationspaket wird im selben Ordner abgelegt.

5. Standardmäßig ist im Schritt **In die Liste mit verwalteten Geräten verschieben** des Assistenten die Option **Geräte nicht verschieben** ausgewählt. Wenn Sie das Client-Gerät nach der Installation des Administrationsagenten nicht in Administrationsgruppen verschieben möchten, ändern Sie die Auswahl der Option nicht.

   Wenn Sie das Client-Gerät nach der Installation des Administrationsagenten verschieben möchten, wählen Sie die Option **Nicht zugeordnete Geräte in diese 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.

6. Wenn die Erstellung des autonomen Installationspakets abgeschlossen ist, klicken Sie auf die Schaltfläche **ABSCHLIESSEN**.

   Der Assistent für das Erstellen eines autonomen Installationspakets wird geschlossen.

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**.

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.

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.

Um den Administrationsagent für Linux im Silent-Modus zu installieren:

1. Bereiten Sie das betreffende Linux-Gerät auf die Remote-Installation vor. Laden Sie mithilfe eines passenden Paket-Management-Systems das deb- oder rpm-Paket des Administrationsagenten herunter und erstellen Sie das Remote-Installationspaket.

2. 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.

3. Lesen Sie den Endbenutzer-Lizenzvertrag. Folgen Sie den unten aufgeführten Schritten nur, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags verstehen und akzeptieren.

4. Geben Sie den Wert der Umgebungsvariablen "KLAUTOANSWERS" an, indem Sie den vollständigen Namen (inklusive Pfad) der Antwort-Datei beispielsweise wie folgt eingeben:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

5. Erstellen Sie die Datei (im txt-Format) in dem Verzeichnis, welches Sie in der Umgebungsvariablen angegeben haben. 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	Notwendig	Beschreibung	M
KLNAGENT_SERVER	Ja	Beinhaltet den Name des Administrationsservers in Form des voll qualifizierten Domänennamens (FQDN) oder der IP-Adresse.	DNS- Adre
KLNAGENT_AUTOINSTALL	Ja	Gibt an, ob der Silent-Modus für die Installation aktiviert ist.	1—De aktiv Benu währ keine Auffo zu tu Ande Modu und d währ Auffo erhal
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 – Ic ich d und E diese Lizer vollst habe und a Ande keine akzep Bedi Endb Lizer (die I nicht
KLNAGENT_PROXY_USE	Nein	Gibt an, ob die Verbindung zum Administrationsserver Proxy-Einstellungen verwendet. Als Standardwert ist 0 vorgegeben.	1—Die Einst verw Ande Einst nicht
KLNAGENT_PROXY_ADDR	Nein	Gibt die Adresse des Proxyservers an, der für die Verbindung mit dem Administrationsserver verwendet wird.	DNS- Adre
KLNAGENT_PROXY_LOGIN	Nein	Gibt den Benutzernamen an, der für die Anmeldung am Proxyserver verwendet wird.	Ein b existi Benu

KLNAGENT_PROXY_PASSWORD	Nein	Gibt Kennwort des Benutzers an, das für die Anmeldung am Proxyserver verwendet wird.	Ein b alpha Zeich Kenn Betri zuläs
KLNAGENT_VM_VDI	Nein	Gibt an, ob der Administrationsagent auf einem Abbild zur Erstellung dynamischer virtueller Maschinen installiert wird.	1—De Admi wird insta ansc Erste virtu genu Ande Insta Abbi
KLNAGENT_VM_OPTIMIZE	Nein	Gibt an, ob die Administrationsagent-Einstellungen optimal für Hypervisor sind.	1—Die lokale Admi Einst ange eine Verw Hype
KLNAGENT_TAGS	Nein	Liste der Tags, die der Instanz des Administrationsagenten zugewiesen wurden.	Ein o Name ein S
KLNAGENT_UDP_PORT	Nein	Gibt den vom Administrationsagenten verwendeten UDP-Port an. Als Standardwert ist 15000 vorgegeben.	Eine existi Portn
KLNAGENT_PORT	Nein	Gibt den vom Administrationsagenten verwendeten Non-TLS-Port an. Als Standardwert ist 14000 vorgegeben.	Eine existi Portn
KLNAGENT_SSLPORT	Nein	Gibt den vom Administrationsagenten verwendeten TLS-Port an. Als Standardwert ist 13000 vorgegeben.	Eine existi Portn
KLNAGENT_USESSL	Nein	Gibt an, ob Transport Layer Security (TLS) für die Verbindung verwendet wird.	1 (Sta verw Ande verw
KLNAGENT_GW_MODE	Nein	Gibt an, ob ein Verbindungsgateway verwendet wird.	1 (Sta aktue wurd (Bein

			kein Verb ange 2—Es verw 3—Es verw 4—Di Admi wird Verb die d (DMZ
KLNAGENT_GW_ADDRESS	Nein	Gibt die Adresse des Verbindungsgateways an. Der Wert wird nur ausgewertet, wenn "KLNAGENT_GW_MODE=3" gesetzt ist.	DNS- Adre
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—Da Regis Benu Gerä nach des Admi ausg Ande
PTCH_ALLOW_APPLY_NONAPROVED_PATCHES	Nein	Legt fest, ob heruntergeladene Updates für den Administrationsagenten mit dem Status *Nicht definiert* automatisch installiert werden sollen.	true Upda auto false nicht insta

6. Administrationsagent installieren:

- Um den Administrationsagenten von einem RPM-Paket auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
  `# rpm -i klnagent-<Build-Nummer>.i386.rpm`

- Um den Administrationsagenten von einem RPM-Paket auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
  `# rpm -i klnagent64-<Build-Nummer>.x86_64.rpm`

- Um den Administrationsagenten von einem RPM-Paket auf einem 64-Bit-Betriebssystem für die ARM-Architektur zu installieren, führen Sie den folgenden Befehl aus:
  `# rpm -i klnagent64-<Build-Nummer>.aarch64.rpm`

- Um den Administrationsagenten von einem DEB-Paket auf einem 32-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
  `# apt-get install ./klnagent_<Build-Nummer>_i386.deb`

- Um den Administrationsagenten von einem DEB-Paket auf einem 64-Bit-Betriebssystem zu installieren, führen Sie den folgenden Befehl aus:
  `# apt-get 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:
  `# apt-get install ./klnagent64_<Build-Nummer>_arm64.deb`

Die Installation des Administrationsagenten für Linux wird im Silent-Modus gestartet und der Benutzer erhält während des Vorgangs keinerlei Aufforderungen, etwas zu tun.

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.

Bevor Sie beginnen:

- Stellen Sie sicher, dass auf dem Gerät, auf dem Sie den Administrationsagenten für Linux installieren möchten, eine der unterstützten Linux-Distributionen ausgeführt wird.

- Laden Sie die erforderliche Installationsdatei für den Administrationsagenten von der Kaspersky-Website herunter.

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_initrafs.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 Programmschlüssel:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Legen Sie den Programmschlüssel "/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg" in das Verzeichnis ab, das Sie im vorherigen Schritt erstellt haben:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

Wenn der Programmschlüssel "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.

6. Führen Sie die Schritte zur Vorbereitung aus, die für jedes Linux-Gerät gelten.

Das Gerät ist vorbereitet. Jetzt können Sie mit der Installation des Administrationsagenten fortfahren.

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.
- **Programmname**. Programmname, der in dem autonomen Installationspaket enthalten ist.
- **Programmversion**.
- **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.
- **Dateihash**. 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.

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:

- Veröffentlichung 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.
- Laden Sie ein autonomes Installationspaket auf Ihr Gerät herunter, 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.

Installationspakete an sekundäre Administrationsserver verteilen

Kaspersky Security Center Linux ermöglicht Ihnen das erstellen von Installationspaketen für Kaspersky-Programme und für Programme 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 **Assets (Geräte)** → **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 **Programm** 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.

Ein Linux-Gerät vorbereiten und den Administrationsagenten auf einem Linux-Gerät remote installieren

Die Installation des Administrationsagenten umfasst zwei Schritte:

- Vorbereitung eines Linux-Geräts
- Remote-Installation des Administrationsagenten

Vorbereitung eines Linux-Geräts

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 Linux-Zielgerät die folgende Software installiert ist:
   - Sudo
   - Perl-Sprachinterpreter ab Version 5.10
2. 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. Deaktivieren Sie das Kennwort der sudo-Abfrage für das Benutzerkonto, das für die Verbindung mit dem Gerät verwendet wird.

c. Verwenden Sie den Befehl `visudo` in sudo, um die Konfigurationsdatei sudoers zu öffnen.

Suche Sie in der geöffneten Datei nach der Zeile, die mit `%sudo` beginnt (bzw. mit `%wheel`, wenn Sie das Betriebssystem CentOS verwenden). Geben Sie unterhalb dieser Zeile Folgendes an: `<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 in der Datei "/etc/sudoers" die letzte Zeile mit dem folgenden Text hinzu: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

d. Speichern und schließen Sie die Datei sudoers.

e. Stellen Sie erneut eine Verbindung zum Gerät über SSH her und stellen Sie mithilfe des Befehls `sudo whoami` sicher, dass der Dienst Sudo kein Kennwort abfragt.

3. Öffnen Sie die Datei `/etc/systemd/logind.conf` file und nehmen Sie folgende Änderungen vor:

- 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`.

Astra Linux-Zielgerät

Wenn auf dem Zielgerät Astra Linux ausgeführt wird, fügen Sie die Zeichenfolge `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.

OSnova-Zielgerät

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
```

4. 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.

5. 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.

Remote-Installation des Administrationsagenten

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. Laden Sie das Installationspaket des Administrationsagenten über die Programmoberfläche oder über die Kaspersky-Website herunter.

   c. 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`.

Die Installation kann fehlerhaft abgeschlossen werden, wenn Sie den Administrationsagenten auf Geräten mit Fedora-Betriebssystemen unter Version 20 mithilfe des SSH-Protokolls installieren. Um den Administrationsagenten in diesem Fall erfolgreich zu installieren, kommentieren Sie in der Datei/etc/sudoers die Einstellung "Defaults requiretty" aus (Setzen Sie es in Kommentar-Syntax, um die Zeile vom zu parsenden Code auszuschließen). Eine ausführliche Beschreibung, warum die Einstellung "Defaults requiretty" Probleme bei der Verbindung über SSH verursachen kann, finden Sie auf der Webseite des Bugzilla Bugtrackers.

Programme mit der Aufgabe zur Remote-Installation installieren

Mit Kaspersky Security Center Linux können Sie Programme 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 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.

Für eine korrekte Ausführung der Aufgabe der Remote-Installation auf einem Gerät, auf dem der Administrationsagent nicht installiert ist, müssen die folgenden Ports geöffnet werden: TCP 139 und 445 sowie UDP 137 und 138. Diese Ports sind standardmäßig auf allen Geräten geöffnet, die zur Domäne gehören. Sie öffnen sich automatisch mithilfe des Tools zur Vorbereitung der Geräte auf die Remote-Installation.

Eines Programm remote installieren

Dieser Abschnitt enthält Informationen darüber, wie ein Programm auf Geräten in einer Administrationsgruppe, auf Geräten mit bestimmten Adressen oder auf einer Auswahl an Geräten remote installiert wird.

Um ein Programm auf ausgewählten Geräten zu installieren:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet.
3. Wählen Sie im Feld **Aufgabentyp** die Variante **Remote-Installation eines Programms** aus.
4. Wählen Sie eine der folgenden Varianten aus:

   - Aufgabe einer Administrationsgruppe zuweisen

     Die Aufgabe wird Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen festlegen oder eine neue erstellen.

     Sie können diese Option beispielsweise zum Starten einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die in einer bestimmten Administrationsgruppe enthalten sind.

   - 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.

Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Vielleicht wollen 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 Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen festlegen.

  Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

Die Aufgabe *Remote-Installation eines Programms* 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 **Installationspakete** die folgenden Einstellungen an:

   - Wählen Sie im Feld **Installationspaket auswählen** das Installationspaket eines Programms, das Sie installieren möchten.

   - Wählen Sie in der Einstellungsgruppe **Download des Installationspakets erzwingen** die Methode der Übertragung der zur Programminstallation 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, ein Windows-Programm (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 also ein Windows-Programm 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 eines Programms* 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 eines Programms* 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 **Kennwort zur Deinstallation der aktuellen Kaspersky-Anwendung** ein Beachten Sie, dass Ihr aktuelles Kaspersky-Programm während der Migration deinstalliert wird.

  Das Feld **Kennwort zur Deinstallation 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 *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 das ausgewählte Programm nicht neu installiert, wenn es bereits auf dem Client-Gerät installiert ist.

    Wenn Sie dieses Kontrollkästchen deaktivieren, wird das Programm in jedem Fall installiert.

    Diese Option ist standardmäßig aktiviert.

  - **Typ des Betriebssystems vor dem Download prüfen**

    Bevor die Dateien auf die Client-Geräte übertragen werden, prüft Kaspersky Security Center Linux, ob die Einstellungen des Installationstools 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 ein Programm 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.

  - **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 Programme zu schließen**

Laufende Anwendungen können das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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 das Programm 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.

7. Geben Sie in diesem Schritt des Assistenten an, ob die Geräte während der Installation von Programm 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 eines Programms* verwendet werden sollen:

   - **Kein Benutzerkonto erforderlich (Administrationsagent ist installiert)**

     Wenn diese Variante ausgewählt ist, muss das Benutzerkonto nicht angegeben werden, unter dem das Installationsprogramm 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 angeben, um das Programm zu installieren.

     Um das Benutzerkonto anzugeben, unter dem das Installationsprogramm ausgeführt werden soll, klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Lokales Benutzerkonto** 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.

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 Aufgaben-Parameter überprüfen, ändern oder bei Bedarf einen Zeitplan für den Start der 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 das ausgewählte Programm auf den angegebenen Geräten installiert.

Programme auf sekundären Administrationsservern installieren

Um ein Programm 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 zum Programm 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 des Programms auf den sekundären Administrationsservern. Wählen Sie den Aufgabentyp **Remote-Installation eines Programms auf sekundärem Administrationsserver** aus.

   Der Assistent für das Hinzufügen einer Aufgabe erstellt eine Aufgabe, mit der das im Assistenten ausgewählte Programm 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 das ausgewählte Programm auf den angegebenen sekundären Administrationsservern installiert.

Einstellungen für die Remote-Installation auf Unix-Geräten angeben

Wenn Sie ein Programm 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 **Assets (Geräte)** → **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 **Programmeinstellungen** → **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 auf dem Zielgerät befindlichen temporären Ordners mit Berechtigungen zur Ausführung von Dateien an (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. Das Programm legt das Installationspaket in dem Verzeichnis ab und führt den Installationsvorgang aus.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Die angegebenen Aufgabeneinstellungen werden gespeichert.

Ersetzen von Sicherheitsanwendungen von Drittanbietern

Zur Installation der Sicherheitsanwendungen von Kaspersky mithilfe von Kaspersky Security Center Linux ist es möglicherweise erforderlich, Drittanbietersoftware zu löschen, die mit dem zu installierenden Programm nicht kompatibel ist. Kaspersky Security Center Linux bietet mehrere Methoden zur Deinstallation von Drittanbieter-Programmen.

Inkompatible Programme während der Konfiguration der Remote-Installation eines Programms entfernen

Sie können die Option **Inkompatible Programme 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 Programme.

Löschen der inkompatiblen Programme mithilfe einer separaten Aufgabe

Zum Löschen der inkompatiblen Programme wird die Aufgabe *Remote-Deinstallation eines Programms* 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 eines Programms* ist.

Die Verwendung dieser Löschmethode ist zweckmäßig, wenn der Installer der Sicherheitsanwendung eines der inkompatiblen Programme nicht erfolgreich löschen kann.

Programme oder Software-Updates remote löschen

Sie können Programme oder Software-Updates auf verwalteten Geräten, auf denen Linux ausgeführt wird, nur per Fernzugriff über den Administrationsagenten entfernen.

Um Programme oder Software-Updates von ausgewählten Geräten remote zu entfernen:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **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 **Programm** die Option "Kaspersky Security Center" aus.

4. Wählen Sie in der Liste **Aufgabentyp** den Typ **Remote-Deinstallation eines Programms** 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. Wählen Sie aus, welche Art von Software Sie entfernen wollen, und wählen Sie anschließend bestimmte Programme, Updates oder Patches aus, die Sie entfernen wollen:

   - **Verwaltetes Programm deinstallieren**

     Eine Liste mit Kaspersky-Programmen angezeigt. Wählen Sie das Programm aus, das Sie entfernen möchten.

   - **Inkompatibles Anwendung deinstallieren**

     Eine Liste mit Programmen, die nicht kompatibel zu Kaspersky-Sicherheitsanwendungen oder zu Kaspersky Security Center Linux sind, wird angezeigt. Aktivieren Sie die Kontrollkästchen neben den Programmen, die Sie entfernen möchten.

   - **Programm aus der Programm-Registry deinstallieren**

Standardmäßig übertragen Administrationsagenten die Information über Programme, die auf verwalteten Geräten installiert sind, an den Administrationsserver. Die Liste der installierten Programme ist in der Programm-Registry. gespeichert.

Um ein Programm von der Programm-Registry auszuwählen:

a. Klicken Sie auf das Feld **Zu deinstallierendes Programm** und wählen Sie anschließend das Programm aus, welches Sie entfernen wollen.

b. Geben Sie die folgenden Optionen für die Deinstallation an:

- Deinstallationsmodus

  Wählen Sie aus, wie Sie das Programm entfernen möchten:

  - **Deinstallationsbefehl automatisch definieren**

    Wenn das Programm einen Deinstallationsbefehl besitzt, welcher durch den Hersteller des Programms vorgegeben wurde, nutzt Kaspersky Security Center Linux diesen Befehl. Es wird empfohlen, diese Option auszuwählen.

  - **Deinstallationsbefehl angeben**

    Wählen Sie diese Option aus, wenn Sie Ihren eigenen Befehl für die Deinstallation des Programms angeben möchten.

    Es wird empfohlen, das Entfernen des Programms zunächst unter Verwendung der Option **Deinstallationsbefehl automatisch definieren** auszuprobieren. Sollte die Deinstallation mittels automatisch definierten Befehl fehlschlagen, verwenden Sie Ihren eigenen Befehl.

    Geben Sie einen Installationsbefehl in das Feld ein und geben Sie anschließend folgende Optionen an:

    Diesen Deinstallationsbefehl nur dann verwenden, wenn der Standardbefehl nicht automatisch entdeckt wurde

    Kaspersky Security Center Linux prüft, ob das ausgewählte Programm einen vom Programmhersteller vorgegeben Deinstallationsbefehl besitzt. Wenn so ein Befehl existiert, verwendet Kaspersky Security Center Linux diesen anstelle des Befehls der in dem Feld **Deinstallationsbefehl des Programms** angegeben wurde.

    Es wird empfohlen, diese Option zu aktivieren.

- Nach einer erfolgreichen Deinstallation einen Neustart durchführen

  Wenn der Vorgang nach einer erfolgreichen Deinstallation einen Neustart des Betriebssystems auf dem verwalteten Gerät benötigt, wird das Betriebssystem automatisch neu gestartet.

- Bestimmtes Programm-Update, einen Patch oder Dritthersteller-Programm deinstallieren

Es wird eine Liste mit Updates, Patches und Drittanbieter-Programmen angezeigt. Wählen Sie das Objekt aus, das Sie entfernen möchten.

Die angezeigte Liste ist eine allgemeine Liste mit Programmen und Updates, die nicht den tatsächlich installierten Programmen und Updates auf den verwalteten Geräten entspricht. Es wird empfohlen, vor der Auswahl eine Objekts zu überprüfen, ob das Programm oder Update tatsächlich auf dem im Aufgabenbereich festgelegten Geräten installiert ist. Sie können sich die Liste mit Geräten, auf denen das Programm oder Update installiert ist, über das Eigenschaftenfenster anzeigen lassen.

Um die Liste der Geräte anzuzeigen:

a. Klicken Sie auf den Namen des Programms oder des Updates.

Daraufhin wird das Eigenschaftenfenster geöffnet.

b. Öffnen Sie den Abschnitt **Geräte**.

Sie können sich die Liste mit installierten Programmen und Updates auch im Eigenschaftenfenster des Geräts anzeigen lassen.

8. Geben Sie an, auf welche Weise Client-Geräte das Tool für die Deinstallation 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**

  Die Option ist veraltet. Verwenden Sie stattdessen die Option **Unter Nutzung des Administrationsagenten** oder **Unter Nutzung von Betriebssystemressourcen durch Verteilungspunkte**.

  Die Dateien werden mit den Betriebssystem-Tools des Administrationsservers 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 den Client-Geräten mithilfe der Tools von den Betriebssysteme durch Verteilungspunkte ausgeliefert. Diese Option kann aktiviert werden, wenn sich im Netzwerk mindestens ein Verteilungspunkt befindet.

  Ist die Option **Unter Nutzung des Administrationsagenten** aktiviert, werden die Dateien nur dann mit den Betriebssystem-Tools zugestellt, wenn die Funktionen des Administrationsagenten nicht verwendet werden können.

- **Maximale Anzahl gleichzeitiger Downloads**

Die erlaubte Maximalanzahl an Client-Geräten, an die der Administrationsserver simultan Dateien ausliefern kann. Je höher die Nummer, umso schneller werden die Programme deinstalliert, aber umso höher ist auch die Auslastung des Administrationsservers.

- **Maximale Anzahl der Deinstallationsversuche**

  Wenn während der Ausführung der Aufgabe *Remote-Deinstallation eines Programms* für Kaspersky Security Center Linux die Anzahl an Deinstallationsversuchen einer Anwendung auf einem verwalteten Gerät nicht innerhalb der Anzahl an Versuchen, die im Parameter angegeben wurde, erfolgreich ist, stoppt Kaspersky Security Center Linux das Ausliefern des Deinstallationstools auf diesem verwalteten Gerät und startet die Installationsaufgabe auf dem Gerät nicht mehr.

  Der Parameter **Maximale Anzahl der Deinstallationsversuche** ermöglicht es Ihnen, die Ressourcen eines verwalteten Geräts zu sparen und den Datenverkehr zu reduzieren (Deinstallation, MSI-Datei ausführen und Fehlermeldungen).

  Wiederholende Versuche zum Start der Aufgabe können auf ein Problem auf dem Gerät hinweisen, dass die Deinstallation verweigert. Der Administrator sollte das Problem innerhalb der angegeben Anzahl an Deinstallationsversuchen lösen und anschließend die Aufgabe neu starten (manuell oder mittels Zeitplan).

  Wenn die Deinstallation nicht abgeschlossen werden kann, ist das Problem unter Umständen nicht lösbar und jeder weitere Aufgabenstart wird als kostspielig im Sinne unnützen Verbrauchs von Ressourcen und Datenverkehr betrachtet.

  Beim Erstellen der Aufgabe wird der Zähler für die Versuche auf `0` gesetzt. Jede Ausführung des Installers, die einen Fehler zurückliefert 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 der **Maximale Anzahl der Deinstallationsversuche** erhöhen und die Aufgabe zu Deinstallation der Anwendung starten. Alternativ können Sie eine neue Aufgabe des Typs *Remote-Deinstallation eines Programms* erstellen.

- **Typ des Betriebssystems vor dem Download prüfen**

  Bevor die Dateien auf die Client-Geräte übertragen werden, prüft Kaspersky Security Center Linux, ob die Einstellungen des Installationstools 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 ein Programm 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.

Wechseln Sie zum nächsten Schritt des Assistenten.

9. Geben Sie Neustart-Einstellungen des Betriebssystems an:

- **Gerät nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) 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 Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

- **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. 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. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten Zeitpunkt für einen Neustart auszuwählen.

  Diese Variante ist standardmäßig ausgewählt.

  - **Aufforderung regelmäßig wiederholen nach (Min.)**
  - **Neu starten nach (Min.)**

- **Beenden von Anwendungen in blockierten Sitzungen erzwingen**

  Laufende Anwendungen können das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

  Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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.

Wechseln 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 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.

Geben Sie das Benutzerkonto an, unter dem das Installationsprogramm gestartet werden soll. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie **Benutzerkonto** 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.

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 **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 bei der Aufgabenerstellung festgelegten Einstellungen ändern.

    Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Liste mit Aufgaben auf den Namen der erstellten Aufgabe klicken.

    Die Aufgabe ist erstellt, konfiguriert und wird in der Aufgabenliste unter **Assets (Geräte)**→ **Aufgaben** angezeigt.

13. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf die Schaltfläche **Starten**.

    Sie können auf der Registerkarte **Zeitplan** im Eigenschaftenfenster der Aufgabe auch einen Zeitplan für den Aufgabenstart festlegen.

    Eine detaillierte Beschreibung der Einstellungen für das Starten nach Zeitplan finden Sie in den allgemeinen Aufgabeneinstellungen.

Nachdem Abschluss der Aufgabe ist ist die ausgewählte Anwendung von allen ausgewählten Geräten deinstalliert.

Ein Gerät mit SUSE Linux Enterprise Server 15 für die Installation des Administrationsagenten vorbereiten

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: Der `Paketheader ist nicht signiert!` Wählen Sie die Option `i`, um die Warnung zu ignorieren.

Nachdem Sie das SUSE Linux Enterprise Server 15-Gerät vorbereitet haben, stellen Sie den Administrationsagenten bereit und installieren ihn.

Ein Windows-Gerät für die Remote-Installation vorbereiten Das Tool "Riprep"

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 erneut gestartet 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 **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 lösen, die bei der Installation des Programms auf dem Client-Gerät aufgetreten sind, auf dem der Administrationsagent nicht installiert wurde, können Sie das Tool Vorbereitung des Geräts auf Remote-Installation (riprep) verwenden.

Verwenden Sie das Tool "riprep", um ein Windows-Gerät für die Remote-Installation vorzubereiten. Um das Tool herunterzuladen, folgen Sie diesem Link: https://media.kaspersky.com/utilities/CorporateUtilities/KSC/riprep.exe

Das Tool Vorbereitung des Geräts auf Remote-Installation wird vom Betriebssystem Microsoft Windows XP Home Edition nicht unterstützt.

Ein Windows-Gerät für die Remote-Installation im interaktiven Modus vorbereiten

Um ein Windows-Gerät auf die Remote-Installation im interaktiven Modus vorzubereiten, gehen Sie wie folgt vor:

1. Starten Sie auf dem Client-Gerät die Datei riprep.exe.
2. Aktivieren Sie im Hauptfenster des Tools zur Vorbereitung einer Remote-Installation die folgenden Optionen:
   - **Deaktivieren des einfachen Zugriffs auf Dateien**
   - **Dienst des Administrationsservers starten**
   - **Ports öffnen**
   - **Benutzerkonto hinzufügen**
   - **Benutzerkontensteuerung (UAC) deaktivieren** (Nur auf Geräten mit den Betriebssystemen Microsoft Windows Vista, Microsoft Windows 7 und Microsoft Windows Server 2008 verfügbar)
3. Klicken Sie auf die Schaltfläche **Starten**.

   Daraufhin werden im unteren Bereich des Hauptfensters des Tools die Etappen der Vorbereitung des Geräts auf die Remote-Installation angezeigt.

Wenn Sie die Option **Benutzerkonto hinzufügen** aktiviert haben, wird beim Erstellen des Benutzerkontos die Aufforderung zur Eingabe eines Benutzerkonto-Namens und eines Kennworts angezeigt. Dadurch wird ein lokales, zur Gruppe lokaler Administratoren gehörendes Benutzerkonto angelegt.

Wenn Sie die Option **Benutzerkontensteuerung (UAC) deaktivieren** aktiviert haben, wird auch dann versucht, die Benutzerkontensteuerung zu deaktivieren, wenn die Benutzerkontensteuerung bereits vor dem Start des Tools deaktiviert wurde. Nach dem Deaktivieren der Benutzerkontensteuerung erscheint auf dem Bildschirm die Aufforderung zum Neustart des Geräts.

Ein Windows-Gerät für die Remote-Installation im Silent-Modus vorbereiten

Um ein Windows-Gerät auf die Remote-Installation im Silent-Modus vorzubereiten, gehen Sie wie folgt vor:

starten Sie auf dem Client-Gerät die Datei riprep.exe aus der Befehlszeile mit den gewünschten Schlüsseln.

Die Befehlszeilensyntax des Tools lautet:

```
riprep.exe [-silent] [-cfg CONFIG_FILE] [-tl traceLevel]
```

Die Schlüssel weisen folgende Bedeutung auf:

- `-silent` – Das Tool im Silent-Modus starten.
- `-cfg CONFIG_FILE` – Konfiguration des Tools definieren, wobei `CONFIG_FILE` der Pfad zur Konfigurationsdatei ist (Datei mit der Erweiterung .ini).
- `-tl traceLevel` – Eingeben der Ablaufverfolgungsebene, wobei `traceLevel` eine Zahl von 0 bis 5 sein kann. Wenn der Schlüssel nicht eingegeben wurde, wird der Wert 0 gesetzt.

Durch das Starten des Tools im Silent-Modus können Sie die folgenden Aufgaben ausführen:

- Einfache Dateifreigabe deaktivieren.
- Dienst Server auf dem Client-Gerät starten.
- Ports öffnen.
- Benutzerkonto anlegen.
- Benutzerkontensteuerung (UAC) deaktivieren.

Sie können die Einstellungen für die Vorbereitung des Geräts auf die Remote-Installation in der Konfigurationsdatei angeben, die mit dem Schlüssel `-cfg` vorgegeben wird. Um diese Einstellungen anzugeben, fügen Sie die folgenden Daten in die Konfigurationsdatei ein:

- Geben Sie im Abschnitt `Common` an, welche Aufgaben ausgeführt werden sollen:
  - `DisableSFS` – Einfache Freigabe von Dateien deaktivieren (0 – Aufgabe ist deaktiviert, 1 – Aufgabe ist aktiviert).
  - `StartServer` – Dienst Server starten (0 – Aufgabe ist deaktiviert, 1 – Aufgabe ist aktiviert).
  - `OpenFirewallPorts` – Alle nötigen Ports öffnen (0 – Aufgabe ist deaktiviert, 1 – Aufgabe ist aktiviert).
  - `DisableUAC` – Benutzerkontensteuerung (UAC) deaktivieren (0 – Aufgabe ist deaktiviert, 1 – Aufgabe ist aktiviert).
  - `RebootType` – Verhalten beim erforderlichen Neustart beim Deaktivieren der Benutzerkontensteuerung definieren Sie können folgende Parameterwerte verwenden:
    - 0 – Gerät nie neu starten.
    - 1 – Gerät neu starten, wenn die Benutzerkontensteuerung vor dem Start des Tools aktiviert wurde.
    - 2 – Gerät zwingend neu starten, wenn die Benutzerkontensteuerung vor dem Start des Tools aktiviert wurde.
    - 4 – Gerät immer neu starten.
    - 5 – Gerät immer zwingend neu starten.
- Geben Sie im Abschnitt `UserAccount` den Benutzerkonto-Namen (`user`) und dessen Kennwort (`Pwd`) ein.

Beispiel für Inhalt einer Konfigurationsdatei:

```
[Common]
DisableSFS=0
```

```
StartServer=1
OpenFirewallPorts=1
[UserAccount]
user=Admin
Pwd=Pass123
```

Nach Abschluss der Ausführung des Tools werden im Startordner die folgenden Dateien erstellt:

- riprep.txt – Bericht über den Verlauf, in dem die Vorgänge des Tools mit Beschreibungen angegeben sind.
- riprep.log – Protokolldatei (wird angelegt, wenn eine Ablaufverfolgungsstufe größer 0 eingegeben wurde).

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 remote zu installieren.

Ein Installationspaket enthält ein zip-Archiv mit einer Reihe von Skripten zur Ausführung auf Client-Geräten und 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. Wechseln Sie zum **Assistent für das Erstellen einer Aufgabe** und wählen Sie den Aufgabentyp **Skripte remote ausführen** ausführen aus.
2. Geben Sie den Aufgabennamen ein und wählen Sie die Geräte aus, denen die Aufgabe zugewiesen werden soll. Klicken Sie auf die Schaltfläche **Weiter**.
3. Wählen Sie ein Installationspaket zur Remote-Ausführung aus, das auf einem zip-Archiv basiert und die "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 der Aufgabe zugewiesene Benutzerkonto zu ändern, beenden Sie die Aufgabe in den Aufgabeneinstellungen und starten Sie diese 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 die Schaltfläche **Fertigstellen**.

   Daraufhin wird die Aufgabe *Remote-Ausführung von Skripten* erstellt und in der Aufgabenliste angezeigt.

Nach dem Abruf der Daten der Aufgabe *Remote-Ausführung von Skripten* 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 Grundlage einer Manifestdatei erstellen

So erstellen Sie ein Installationspaket auf Grundlage einer Manifestdatei:

1. Führen Sie eine der folgenden Aktionen aus:

   - Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.
   - Wechseln Sie im Hauptmenü zu **Vorgänge → Datenverwaltung → Installationspakete**.

   Eine Liste der auf dem Administrationsserver verfügbaren Installationspakete wird angezeigt.

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 **Erstellen Sie für die Aufgabe "Skripte remote ausführen" ein Installationspaket, dass auf einer zip-Datei basiert, in welcher die Datei "manifest.json" enthalten ist** aus.

4. Geben Sie den Namen des Pakets an und klicken Sie auf die Schaltfläche **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.

   Es wird damit begonnen, die Datei auf den Kaspersky Security Center Linux Administrationsserver hochzuladen.

   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 hochgeladen. Nach Abschluss des Hochladens wird das Installationspaket in der Liste der Installationspakete angezeigt.

Wenn Sie in der Liste der auf dem Administrationsserver verfügbaren Installationspakete auf den Link mit dem Namen eines benutzerdefinierten Installationspakets klicken, können Sie:

- Anzeigen der folgenden Eigenschaften eines Installationspakets:
  - **Name.** Der Name des benutzerdefinierten Installationspakets.

- **Quelle.** Der Programmhersteller.
- **Version.** Programmversion.
- **Erstellt.** Erstellungsdatum des Installationspaketes.
- **Geändert.** Änderungsdatum des Installationspaketes.
- **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 Manifest-Datei und Beschreibung der Arrays

JSON-Schema

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema der Aufgabe zum Starten von Skripten",
   "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 Manifest-Datei

```
{
 "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`

<Datei1>

<Datei2>

<Ordner1>/<Datei3>

<Ordner2>/<Ordner3>/<Datei4>

...

<DateiX>

Die Datei "manifest.json" ist die Manifestdatei für die Aufgabe.

<Datei1>, ..., <DateiX> entspricht den Dateien mit auszuführenden Skripten.

Anwendungen auf Geräten mittels Aufgabe zur Remote-Ausführung von Skripten installieren

Die Aufgabe *Skripte remote ausführen* kann dazu verwendet werden, eine Anwendung auf einem Client-Gerät remote zu installieren, indem ein benutzerdefiniertes Installationspaket erstellt wird.

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:

- <Paktename>.deb
- **install.sh**

  ```
  sudo dpkg -I <Paketname>.deb
  ```

- **manifest.json**

JSON-Schema für die Remote-Installation einer Anwendung

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<enter the arguments, if necessary>",
      "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 übergeben werden.

   d. `results` – Array, das abhängig vom Ergebnis der Aufgabe weitere Aktionen definiert.

      1. `code` – Wert, der ein Skript zurückgibt.

      2. `next` – Aktion, die als nächstes 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 den `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 manifest.json-Datei. 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 Speicher-Verhalten von Ereignissen und die Benachrichtigungen konfigurieren.

So zeigen Sie den Status der Aufgabe Skripte remote ausführen an:

1. Wechseln Sie im Hauptmenü zu **Geräte** → **Aufgaben**.

   Die Aufgabenliste wird angezeigt.

2. Wählen Sie die Aufgabe aus und klicken Sie auf **Geräteverlauf**.

   Der Aufgabenfortschritt wird angezeigt.

So konfigurieren Sie das Speicher-Verhalten von Ereignissen:

1. Klicken Sie in der Aufgabenliste auf die Aufgabe und wechseln Sie zur Registerkarte **Einstellungen**.
2. Klicken Sie im Abschnitt **Benachrichtigungen** auf die Schaltfläche **Einstellungen**.
3. Wählen Sie aus, wie sich die Awendung 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 Datenbank des Administrationsservers, im Ereignisprotokoll des Administrationsservers 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-Programme

Über die Lizenzierung 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 das Programm.

Bitte lesen Sie sich den Endbenutzer-Lizenzvertrag sorgfältig durch, bevor Sie das Programm 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 Programminstallation dem Text des Endbenutzer-Lizenzvertrags zustimmen, gelten die Bedingungen des Endbenutzer-Lizenzvertrags als akzeptiert. Falls Sie den Lizenzvertrag ablehnen, brechen Sie die Programminstallation ab und nutzen Sie das Programm 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 das Programm verwendet wird.

Es sind folgende Lizenztypen vorgesehen:

- *Test*

  Eine kostenlose Lizenz zum Kennenlernen des Programms. Eine Testlizenz verfügt in der Regel über eine kurze Gültigkeitsdauer.

  Nachdem die Gültigkeit einer Testlizenz abgelaufen ist, stellt Kaspersky Security Center Linux die Funktion ein. Um das Programm weiter nutzen zu können, müssen Sie eine kommerzielle Lizenz erwerben.

  Das Programm kann nur einmal im Rahmen einer Testlizenz verwendet werden.

- *Kommerziell*

  Eine kostenpflichtige Lizenz.

  Wenn eine kommerzielle Lizenz abläuft, werden wichtige Programmfunktionen deaktiviert. Zur weiteren Nutzung von Kaspersky Security Center ist eine Verlängerung der kommerziellen Lizenz erforderlich. Nach Ablauf einer kommerziellen Lizenz können Sie das Programm 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:

- Lizenzschlüssel oder Bestellnummer
- Informationen über den Benutzer, dem die Lizenz ausgestellt wird
- Informationen über das Programm, das mit der ausgestellten Lizenz aktiviert werden kann
- Maximale Anzahl von Lizenzeinheiten (z. B. Geräte, auf denen das Programm 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 das Programm aktivieren können, um es 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 im Programm hinzugefügt haben, wird er auf 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 des Programms 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 Testlizenz kann als aktiver Lizenzschlüssel hinzugefügt werden. Der Lizenzschlüssel für eine Testlizenz 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 das Programm aktiviert wird oder nachdem die kommerzielle Lizenz abläuft. Das Programm Kaspersky Security Center, das 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 Programme, 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 Programmen • Einstellungen der auf den Client-Geräten installierten Programme zentral anpassen • Status der Antiviren-Sicherheit eines Unternehmens kontrollieren • Benutzerrollen verwalten • Statistiken und Berichte über die Ausführung von Programmen 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 • Vorhandene lizenzierte Programmgruppen anzeigen und ändern • Liste der durch eine Netzwerkabfrage gefundenen Geräte anzeigen und manuell bearbeiten • Liste der Betriebssystem-Abbilder anzeigen, die für die Remote-Installation verfügbar sind		
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 die Software von Drittanbietern, die auf den verwalteten Geräten installiert ist. • Aufgabe *Schwachstellen schließen* Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für Microsoft-Programme und die benutzerdefinierten Korrekturen für Drittanbieter-Programme. Um die Aufgabe zu verwenden, müssen Sie manuell benutzerdefinierte Korrekturen angeben.	✓	✓
Schwachstellen- und Patch-Management: Erweiterte Funktionen	–	✓

Sie können Regeln für die automatische Remote-Installation von Software-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 Programmen von Kaspersky 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.	✓	✓
Exportieren von Ereignissen in SIEM-Systeme: QRadar von IBM und ArcSight von Micro Focus Der Ereignisexport kann in zentralisierten Systemen verwendet werden, 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 Apps im Echtzeitbetrieb gewährleisten, sowie Security Operation Center (SOC). Unter einen speziellen Lizenz können die Protokolle CEF und LEEF verwendet werden, um allgemeine Ereignisse und Ereignisse, die von Kaspersky-Programmen an den Administrationsserver übertragen werden, in SIEM-Systeme zu exportieren. 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 (Common Event Format) ist ein offener Standard für Protokollierung, 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. Die SIEM-Systeme von ArcSight und Splunk verwenden dieses Protokoll.	–	✓

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 das Programm 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

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-Programmen 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-Programmen auf Geräten
- Verwalten der Einstellungen und Aufgaben von installierten Programmen
- Verwalten der Updates für Programme von Kaspersky und Drittanbietern sowie Auffinden und Schließen von Schwachstellen
- Aktivieren von Kaspersky-Programmen auf Geräten
- Benutzerkonten verwalten
- Anzeigen von Informationen zum Betrieb von Kaspersky-Programmen auf Geräten
- Anzeigen von Berichten

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 Scannen von Active Directory- oder Samba-Domänencontrollern oder durch das Scannen von IP-Intervallen erhalten wurden. Der Administrationsserver ruft unabhängig Daten ab oder empfängt Daten vom Administrationsagent.

- Informationen aus Active Directory und Samba über Organisationseinheiten, Domänen, Benutzer und Gruppen. 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-Programmen, 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.

- Einzelheiten zu den auf dem Gerät installierten Anwendungen von Kaspersky. Die verwaltete Anwendung überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver:

  - Einstellungen der auf dem verwalteten Gerät installierten Kaspersky-Programme: Name und Version des Kaspersky-Programms, 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 Programmkomponenten, Details zu den Einstellungen und Aufgaben von Kaspersky-Programmen, Informationen zu aktiven und Reserve-Lizenzschlüsseln, Installationsdatum der Anwendung und ID.

  - Statistiken zur Anwendungsoperation: Ereignisse im Zusammenhang mit Statusveränderungen von Komponenten der Kaspersky-Programme auf dem verwalteten Gerät und im Zusammenhang mit der

Ausführung von Aufgaben, die von den Softwarekomponenten ausgelöst werden.

- Der Status des Geräts wird von dem Kaspersky-Programm bestimmt.
- Von dem Kaspersky-Programm zugewiesene Tags.

- Daten, die in Ereignissen der Komponenten von Kaspersky Security Center Linux und der durch Kaspersky verwalteten Programmen 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 Daten in die Verwaltungskonsole oder in Kaspersky Security Center Web Console ein.
- Einstellungen der Komponenten von Kaspersky Security Center Linux und der durch Kaspersky verwalteten Programme 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 Programme. 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).
  - 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-Software, 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 Programmen von Drittanbietern 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. 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 verschlüsselte Windows-basierte Geräte und den Verschlüsselungsstatus. Das verwaltete Programm überträgt die Daten von dem Gerät über den Administrationsagenten auf den Administrationsserver.
- Details zu Fehlern bei Datenverschlüsselungen auf Windows-basierten Geräten, die mit der Funktion zur Datenverschlüsselung von Kaspersky-Programmen ausgeführt 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 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 des entsprechenden Programms.

- Informationen über verschlüsselte Geräte und den Verschlüsselungsstatus. Ein verwaltetes Programm 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-Programme 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 Programms.

- 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 des entsprechenden Programms.

- Informationen über Versuche von Unternehmensmitarbeitern, auf Cloud-Dienste zuzugreifen. 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 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.

- Details der eingegebenen Aktivierungscodes und Schlüsseldateien. Der Benutzer gibt Daten in die Verwaltungskonsole oder in die Benutzeroberfläche von 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 zweistufige Überprüfung. 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 Datenbank des Administrationsservers 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 dem durch Kaspersky verwalteten Programm abgerufenen Daten und überträgt sie an den Administrationsserver. Die Liste der verarbeiteten Daten von den durch Kaspersky verwalteten Programmen finden Sie in der Hilfe der entsprechenden Programme.
- Der Administrationsserver bezieht die Informationen über die vernetzten Geräte entweder selbst oder erhält sie von einem Administrationsagenten, der als Verteilungspunkt fungiert.

Die aufgelisteten Daten werden in der Datenbank des Administrationsservers gespeichert. Benutzernamen und Kennwörter werden in verschlüsselter Form 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 folgen der Links in der Verwaltungskonsole oder 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 des Programms 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 des Programms 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 das Programm 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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-Programme

Dieser Abschnitt beschreibt die Funktionen von Kaspersky Security Center, die sich auf die Arbeit mit den Lizenzschlüsseln von verwalteten Kaspersky-Programmen beziehen.

Kaspersky Security Center Linux ermöglicht eine zentrale Verteilung von Lizenzschlüsseln für Kaspersky-Programme 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 das Programm 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-Programme muss mit einer Schlüsseldatei oder einem Aktivierungscode lizenziert werden. Eine Schlüsseldatei oder ein Aktivierungscode kann folgendermaßen bereitgestellt werden:

- Mittels automatischer Verteilung
- Mittels Installationspaket des verwalteten Programms
- Mittels der Aufgabe "Lizenzschlüssel hinzufügen" für ein verwaltetes Programm
- Mittels manueller Aktivierung eines verwalteten Programms

Sie können mit einer der oben aufgeführten Methoden einen neuen aktiven Lizenzschlüssel oder einen Reserve-Lizenzschlüssel hinzufügen. Kaspersky-Programme verwenden zum aktuellen Zeitpunkt einen aktiven Schlüssel und speichern einen Reserveschlüssel, der nach Ablauf des aktiven Schlüssels angewendet wird. Das Programm, für welches 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 Programme 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. Das Programm 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 dieses Programm 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 eines verwalteten Programms

Diese Option wird aus Sicherheitsgründen nicht empfohlen. Eine Schlüsseldatei oder ein Aktivierungscode, der zum Installationspaket hinzugefügt wurde, kann kompromittiert werden.

Wenn die Installation des verwalteten Programms mithilfe eines Installationspakets erfolgt, können Sie eine Schlüsseldatei oder einen Aktivierungscode im Installationspaket oder in der Richtlinie dieses Programms 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 ein verwaltetes Programm

Wenn Sie die Aufgabe zum Hinzufügen eines Lizenzschlüssels für verwaltete Programme 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 das installierte Kaspersky-Programm lokal mithilfe der Tools der Programmoberfläche aktivieren. Weitere Informationen finden Sie in der Dokumentation zum installierten Programm.

Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen

Um einen Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzuzufügen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.
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.
   - **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 "Schlüssel hinzufügen".

Vor der Verteilung müssen Sie den Lizenzschlüssel zur Datenverwaltung des Administrationsservers hinzufügen.

So verteilen Sie einen Lizenzschlüssel an Client-Geräte mittels der Aufgabe "Schlüssel hinzufügen":

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **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 **Programm** das Programm aus, für das Sie einen Lizenzschlüssel hinzufügen möchten.
4. Wählen Sie in der Liste **Aufgabentyp** die Aufgabe **Schlüssels hinzufügen** aus.
5. Geben Sie im Feld **Aufgabenname** den Namen der neuen Aufgabe an.
6. Wählen Sie die Geräte, denen die Aufgabe zugewiesen werden soll.

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 "Schlüssel hinzufügen" 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 den Tabelle mit Schlüsseln den Lizenzschlüssel aus.

10. Aktivieren Sie im Schritt **Lizenzinformationen** des Assistenten die Option **Als Reserveschlüssel verwenden**, wenn Sie diesen Schlüssel als Reserveschlüssel verwenden möchten.

    In diesem Fall wird der hinzugefügte Schlüssel als Reserveschlüssel verwendet, wenn der aktive Schlüssel abgelaufen ist.

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 **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 bei der Aufgabenerstellung festgelegten Einstellungen ändern.

    > Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Liste mit Aufgaben auf den Namen der erstellten Aufgabe klicken.

    Die Aufgabe ist erstellt, konfiguriert und wird in der Aufgabenliste angezeigt.

13. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf die Schaltfläche **Starten**.

    Sie können auf der Registerkarte **Zeitplan** im Eigenschaftenfenster der Aufgabe 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. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.
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**.
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 das Programm 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 dieses Programm 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 manuell einen Lizenzschlüssel verteilen.

Informationen zu verwendeten Lizenzschlüsseln anzeigen

Um die Liste mit Lizenzschlüsseln anzuzeigen, die zur Datenverwaltung des Administrationsservers hinzugefügt wurden, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **Vorgänge → Lizenzierung → Lizenzen für Kaspersky-Software**.

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 für Kaspersky-Software**.
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

Um zu sehen, welche Lizenzschlüssel auf einem bestimmten Client-Gerät bereitgestellt werden, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte) → Verwaltete Geräte**.
2. Klicken Sie auf den Namen des gewünschten Geräts.
3. Wählen Sie im folgenden Eigenschaftenfenster des Geräts die Registerkarte **Programme** aus.
4. Klicken Sie auf den Namen des Programms, für das Sie Informationen über den Lizenzschlüssel anzeigen möchten.

5. Wählen Sie im folgenden Fenster mit den Programmeigenschaften 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 das Programm öffentliche DNS-Server.

Ereignisse bei Überschreitung der Lizenzbeschränkung

Kaspersky Security Center Linux ermöglicht das automatische Empfangen von Informationen über Ereignisse der Überschreitung der Lizenzbeschränkung von Kaspersky-Programmen, 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 das Einstellungen-Symbol ( ) neben dem Administrationsserver.

   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. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.

3. Wählen Sie die erforderliche Schlüsseldatei oder den Aktivierungscode aus und klicken Sie anschließend auf die Schaltfläche **Löschen**.

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 jedes verwaltete Kaspersky-Programm widerrufen. Vor dem Widerruf der EULA müssen Sie das ausgewählte Programm deinstallieren.

So widerrufen Sie eine EULA für verwaltete Kaspersky-Programme:

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.

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 das Kaspersky-Programm 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 das Programm ist deinstalliert.

Lizenzen für Programme von Kaspersky verlängern

Lizenzen für Kaspersky-Programme, 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:

   - Wechseln Sie im Hauptmenü zu **Vorgänge** → **Lizenzierung** → **Lizenzen für Kaspersky-Software**.
   - Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard** und klicken Sie anschließend auf den Link **Ablaufende Lizenzen anzeigen** neben einer Benachrichtigung.

   Es öffnet sich das Fenster **Lizenzen für Kaspersky-Software**, 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. Wechseln 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-Programme 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-Programme**

   Zur Konfiguration und Verteilung der Einstellungen für auf den verwalteten Geräten installierte Kaspersky-Programme 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-Programmen 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-Programme zu verwalten.

3. **Ereignismenge für Datenbank einschätzen und einschränken**

   Informationen über Ereignisse in der Funktionsweise der verwalteten Programme werden vom Client-Gerät übertragen und in der Datenbank des Administrationsservers 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-Programmen, den Aufgaben und der vom Administrationsserver empfangenen Ereignissen geschützt sein.

- Die Kaspersky-Programme werden entsprechend den Richtlinien und Richtlinienprofilen konfiguriert.
- Die Programme 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 Kaspersky-Datenbanken und -Programme 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 Programmeinstellungen zuweisen. Als Ergebnis erhält bei der benutzerorientierten Sicherheitsverwaltung jede Abteilung – die Buchhaltung und die Personalabteilung – eine eigene Konfiguration der Einstellungen für Kaspersky-Programme. Die Konfiguration der Einstellungen legt fest, welche Programmeinstellungen 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 Programmrichtlinie 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 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 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 Programme von Kaspersky umfasst die folgenden Schritte:

1. **Programmrichtlinien anpassen**

   Passen Sie die Einstellungen der auf den verwalteten Geräten installierten Kaspersky-Programme an, indem Sie für jedes Programm 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 Programme:

   - 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 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. **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-Programme, 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-Programme 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-Programme gemäß den festgelegten Einstellungen konfiguriert und mittels Richtlinienhierarchie weitergegeben.

Die konfigurierten Programmrichtlinien 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 Programme von Kaspersky, 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 Programme von Kaspersky umfasst die folgenden Schritte:

1. **Programmrichtlinien anpassen**

   Passen Sie die Einstellungen der auf den verwalteten Geräten installierten Kaspersky-Programme an, indem Sie für jedes Programm 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 Programmeinstellungen 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 Programmfunktionen.

   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 Programme 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-Programme 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-Programme 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 Programme von Kaspersky 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 Programmrichtlinien und Richtlinienprofile werden automatisch auf die Geräte dieses Benutzers angewendet.

Richtlinien und Richtlinienprofile

In Kaspersky Security Center Web Console können Sie Richtlinien für Apps von Kaspersky 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 Kaspersky-Programmeinstellungen, die auf eine Administrationsgruppe und deren Untergruppen angewendet werden. Sie können mehrere Kaspersky-Programme auf den Geräten einer Administrationsgruppe installieren. Kaspersky Security Center bietet eine einzelne Richtlinie für jedes Kaspersky-Programm 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 ein Kaspersky-Programm aktiv sein. Geräte wenden die Einstellungswerte einer aktiven Richtlinie für ein Kaspersky-Programm 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 ein einzelnes Programm können mehrere Richtlinien mit unterschiedlichen Werten konfiguriert werden.
- Für das aktuelle Programm 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 lokale Programmeinstellungen 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 ein Sperrschaltflächensymbol (). Die folgende Tabelle zeigt den Status der Sperrschaltfläche:

Status der Sperrschaltfläche

Status	Beschreibung
Nicht definiert	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 verwalteten Programmoberfläche ändern. Diese Art von Einstellungen wird als *entsperrt* bezeichnet.
Erzwingen	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 eines verwalteten Programms 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-Programmen auf verwalteten Geräten geändert werden.

Sie können eine Sperrschaltfläche verwenden, um die folgenden Aktionen auszuführen:

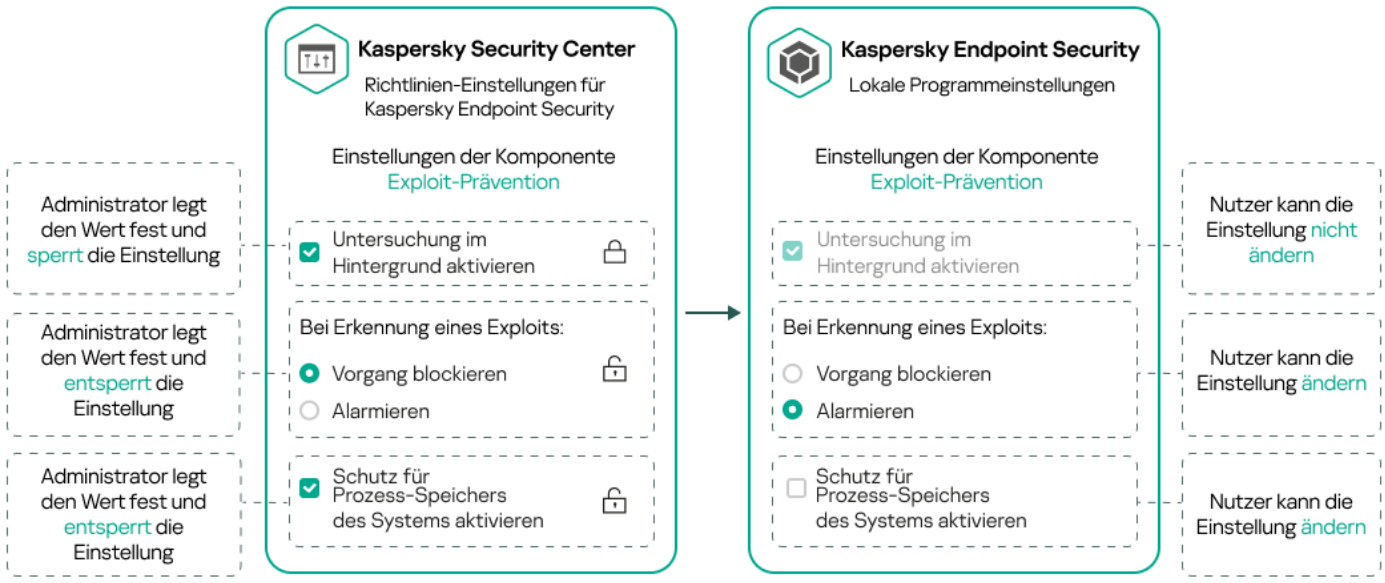
- Sperren von Einstellungen für eine Verwaltungsuntergruppenrichtlinie
- Sperren von Einstellungen eines Kaspersky-Programms auf einem verwalteten Gerät

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 ein verwaltetes Kaspersky-Programm enthalten dieselben Einstellungen. Wenn Sie Richtlinieneinstellungen konfigurieren, ändern die Einstellungen des Kaspersky-Programms die Werte auf einem verwalteten Gerät. Sie können gesperrte Einstellungen auf einem verwalteten Gerät nicht anpassen (siehe Abbildung unten):



Einzelheiten zu den Einstellungen der Kaspersky-Programme

Vererbung von Richtlinien und Richtlinienprofilen

Dieser Abschnitt enthält Informationen zur Hierarchie und Vererbung von Richtlinien und Richtlinienprofilen.

Hierarchie der Richtlinien

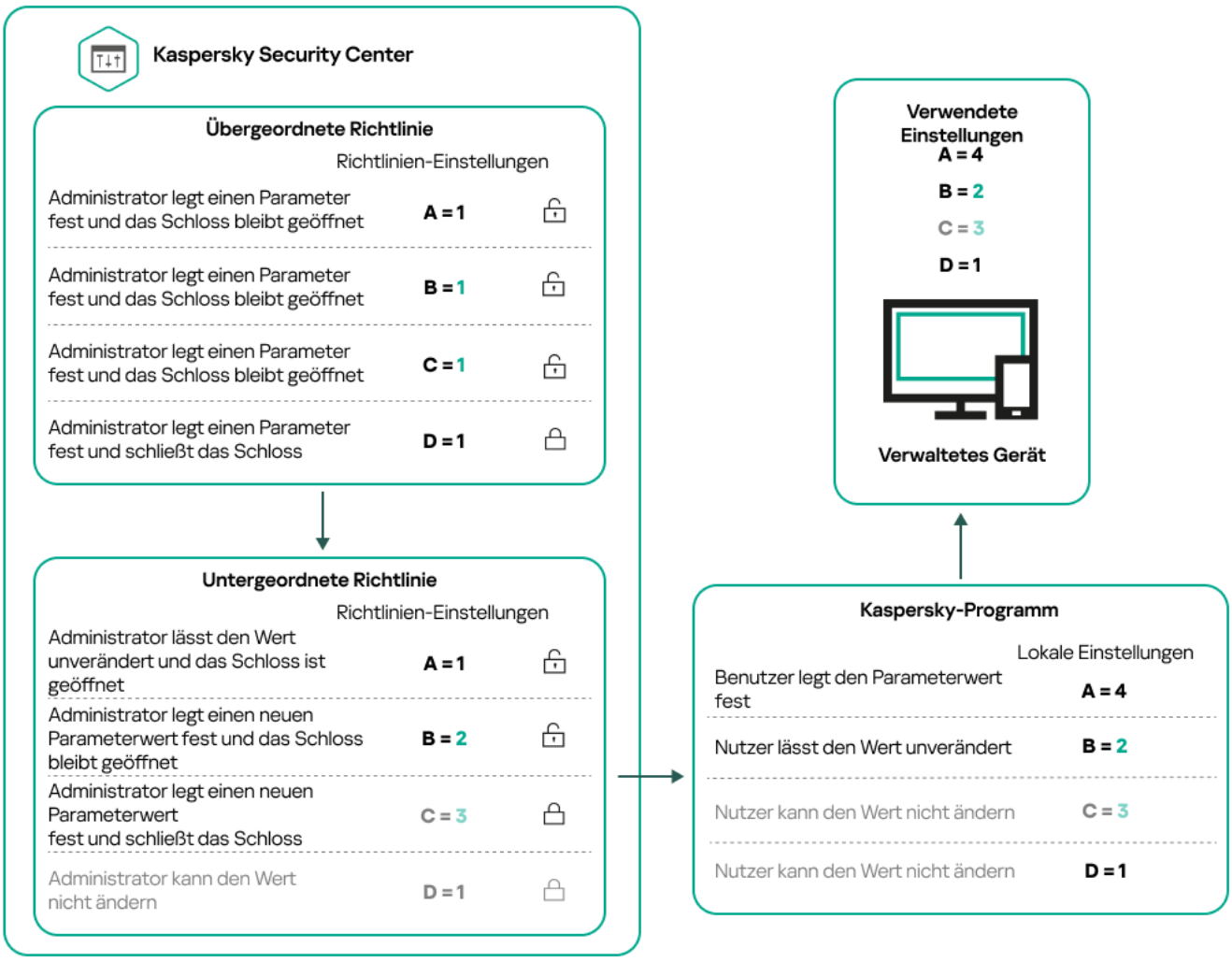
Wenn unterschiedliche Geräte unterschiedliche Einstellungen benötigen, können Sie Geräte in Administrationsgruppen organisieren.

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 desselben Programms 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).

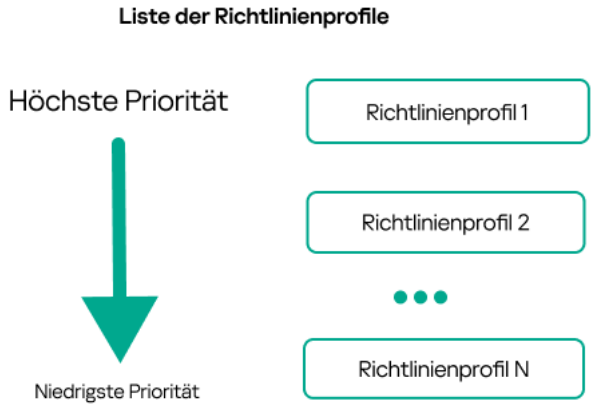


Hierarchie der Richtlinien

Richtlinienprofile in einer Hierarchie von Richtlinien

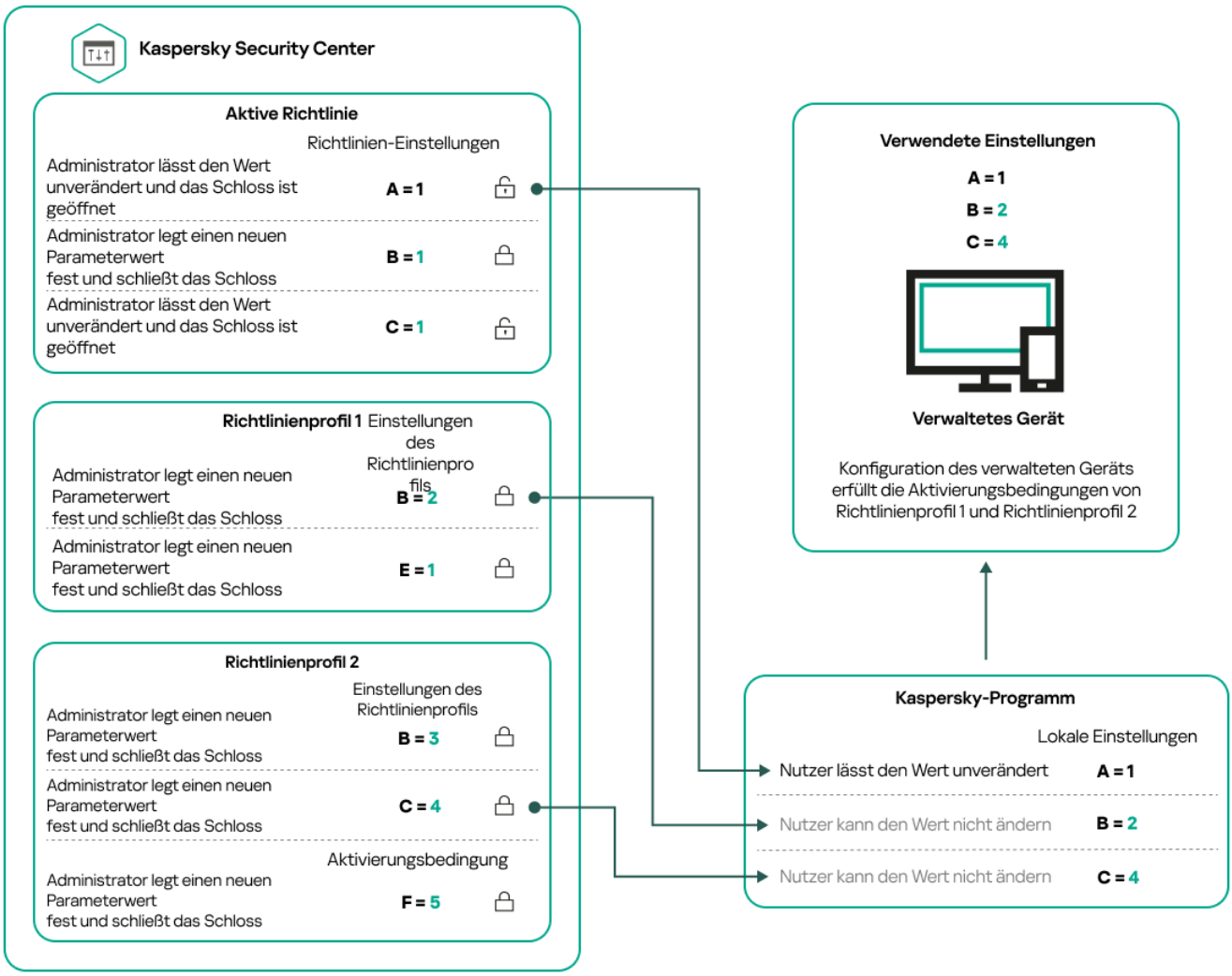
Richtlinienprofile haben die folgenden Bedingungen für die Prioritätszuweisung:

- 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).



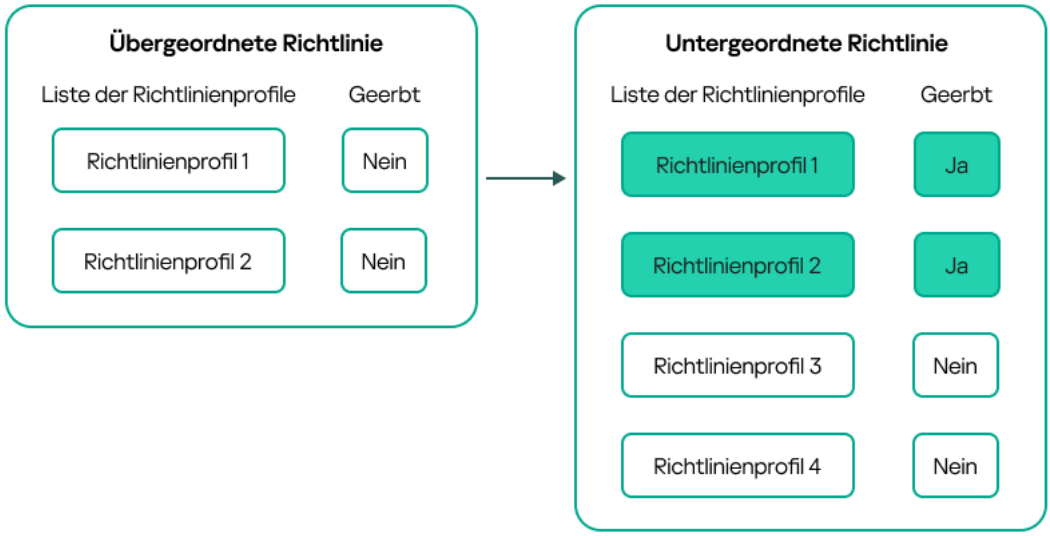
Die Konfiguration des verwalteten Geräts erfüllt die Aktivierungsbedingungen mehrerer Richtlinienprofile.

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).

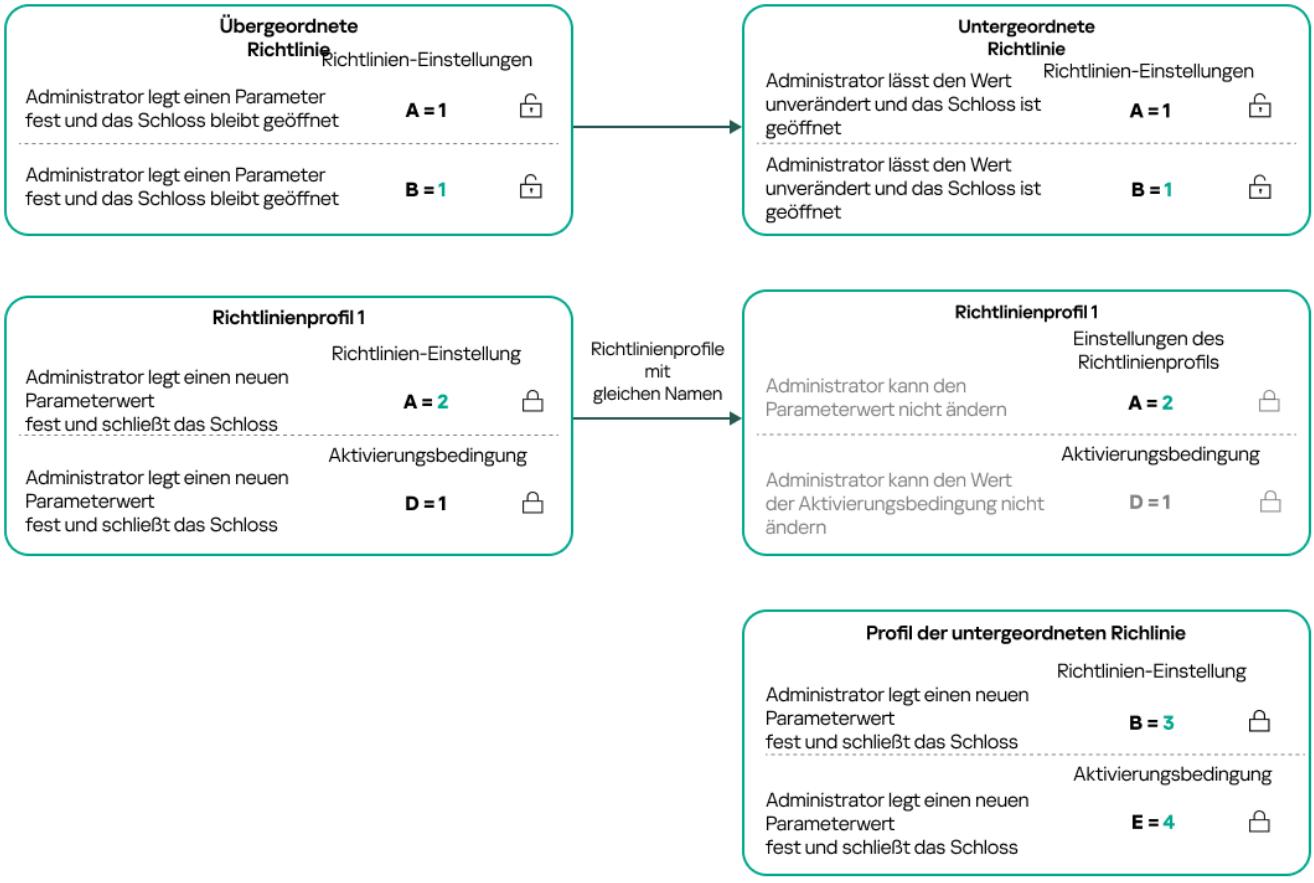


Vererbung von Richtlinienprofilen

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 des verwalteten Programms 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. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **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 **Assets (Geräte)** → **Richtlinien und Profile**.

2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Das Fenster **Programm auswählen** wird geöffnet.

3. Wählen Sie das Programm aus, für das Sie eine Richtlinie erstellen möchten.

4. Klicken Sie auf die Schaltfläche **Weiter**.

   Das Fenster für neue Richtlinieneinstellungen wird geöffnet, in dem die Registerkarte **Allgemein** ausgewählt ist.

5. Ändern Sie gegebenenfalls Standardname, Standardstatus und Standardvererbungseinstellungen der Richtlinie.

6. Wählen Sie die Registerkarte **Programmeinstellungen** 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.

7. Wählen Sie auf der Registerkarte **Programmeinstellungen** 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 welches Programm 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.

8. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

Die Richtlinie wird in der Liste der Richtlinien angezeigt.

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 **Einstellungen erben** 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.

  - Vererben der Einstellungen für 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.

Revisionsverlauf

Auf der Registerkarte **Revisionsverlauf** können Sie eine Liste mit Revisionen der Richtlinie anzeigen 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 **Assets (Geräte)** → **Richtlinien und Profile**.
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 des Programms 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**.

Die Änderungen der Richtlinie werden in den Eigenschaften der Richtlinie gespeichert und im Abschnitt **Revisionsverlauf** angezeigt.

Option zur Vererbung einer Richtlinie aktivieren und deaktivieren

So aktivieren oder deaktivieren Sie die Vererbungsoption in einer Richtlinie:

1. Öffnen Sie die erforderliche Richtlinie.
2. Öffnen Sie die Registerkarte **Allgemein**.
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 **Vererben der Einstellungen für 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.
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 **Assets (Geräte)** → **Richtlinien und Profile**.

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.

Um eine Richtlinie zu einer anderen Administrationsgruppe zu verschieben, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.

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 **Assets (Geräte)** → **Richtlinien und Profile**.
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.

   
   Das Fenster "Richtlinien und Profile" mit der ausgewählten Richtlinie.

   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 **Assets (Geräte)** → **Richtlinien und Profile**.
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 erfolgreichem 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 **Assets (Geräte)** → **Verwaltete 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:
   - Gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**, klicken Sie auf den Pfad-Link im Feld **Aktueller Pfad** über der Liste der verwalteten Geräte und wählen Sie anschließend die Administrationsgruppe aus, welche die zu synchronisierenden Geräte enthält.
   - Führen Sie eine Geräteauswahl durch, um die Geräteliste anzuzeigen.
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**.

   Das Programm 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 ein Kaspersky-Programm 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 Programmrichtlinie an ein verwaltetes Gerät übermittelt wurde:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete 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 **Programme**.
4. Wählen Sie das Programm aus, für das Sie das Datum der Richtliniensynchronisierung anzeigen möchten.

   Das Fenster mit der Programmrichtlinie 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 Übernahmestatus einer Richtlinie für jedes Gerät in einem Statusdiagramm zur Richtlinienverteilung anzeigen.

Um das Statusdiagramm für die Richtlinienverteilung für jedes Gerät anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, für die Sie den Verteilungsstatus auf dem Gerät anzeigen wollen.
3. Wählen Sie im sich öffnenden Menü den Link **Verteilung**.

   Das Fenster **<Name der Richtlinie> Ergebnisse der Verteilung** wird geöffnet.
4. Im geöffneten 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. Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **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**.

   Ihre Einstellungen werden gespeichert und übernommen.

Richtlinie nach dem Ereignis "Virenangriff" automatisch aktivieren

Damit eine Richtlinie beim Eintritt eines Ereignisses "Virenangriff" automatisch aktiviert wird, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Fenster für die Einstellungen des Administrationsservers wird geöffnet und Registerkarte **Allgemein** ist ausgewählt.

2. Wählen Sie den Bereich **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 für die Komponente, die den Virenangriff erkannt hat – Anti-Virus für Workstations und Server, Antiviren-Programme für E-Mail-Systeme, 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 Richtungspfeil (>) neben **Verwaltete Geräte**.

   Eine Hierarchie der Administrationsgruppen und ihrer Richtlinien wird angezeigt.

6. Klicken Sie in der Hierarchie der Administrationsgruppen und ihrer Richtlinien auf die Namen der Richtlinien, die aktiviert werden, wenn ein Virenangriff erkannt wird.

   Um sämtliche Richtlinien in der Liste oder in einer Gruppe auszuwählen, aktivieren Sie das Kontrollkästchen neben dem benötigten Namen.

7. Klicken Sie auf die Schaltfläche **Speichern**.

   Das Fenster mit der Hierarchie der Administrationsgruppen und ihrer Richtlinien wird geschlossen.

Die ausgewählten Richtlinien werden in die Liste der Richtlinien aufgenommen, die aktiviert werden, wenn ein Virenangriff erkannt wird. Die ausgewählten Richtlinien werden bei einem Virenangriff 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 **Assets (Geräte)** → **Richtlinien und Profile**.
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.

Richtlinienprofile verwalten

Dieser Abschnitt beschreibt die Verwaltung von Richtlinienprofilen und enthält Informationen zum Anzeigen der Profile einer Richtlinie, zum Ändern einer Richtlinienprofilpriorität, zum Erstellen eines Richtlinienprofils, zum Kopieren eines Richtlinienprofils, zum Erstellen einer Richtlinienprofilaktivierungsregel und zum Löschen eines Richtlinienprofils.

Profile einer Richtlinie anzeigen

So zeigen Sie Profile einer Richtlinie an:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
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.

Priorität eines Richtlinienprofils ändern

Um die Priorität eines Richtlinienprofils zu ändern, 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, 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.

4. Wählen Sie die Registerkarte **Programmeinstellungen** 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 **Programmeinstellungen** 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.

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.

- **Die Regel für die Verbindung des Administrationsservers ist auf diesem Gerät aktiv**

  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:

  - **Arbeitsspeichergröße (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 Rollenzuordnung**

  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 die Verwendung von 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.

- **Auf Geräte ohne angegebene Tags anwenden**

  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.

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.

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 Programme, die auf Geräten untergeordneter Gruppen installiert sind, unterbunden.

Richtlinieneinstellungen des Administrationsagenten

Gehen Sie folgendermaßen vor, um die Richtlinieneinstellungen des Administrationsagenten anzupassen:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
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.

Bedenken Sie, dass für Geräte auf Basis von Linux und Windows jeweils unterschiedliche Einstellungen zur Verfügung stehen.

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 **Einstellungen erben** 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.
  - **Vererben der Einstellungen für 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 2 GB beträgt (es sind mindestens 4 GB erforderlich, um Programme 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.

Programmeinstellungen

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.

- **Dem Programm 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 oder der Richtlinie für mobile Benutzer, als die Richtlinie an das verwaltete Gerät zugestellt wurde
  - 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

    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 das Kennwort für das Tool "klmover" und für die Aufgabe zur Remote-Deinstallation des Administrationsagenten angeben. Klicken Sie dazu auf die Schaltfläche **Ändern**.

  Diese Option ist standardmäßig deaktiviert.

Datenverwaltung

Im Abschnitt **Datenverwaltung** können Sie die Objekttypen auswählen, deren Daten vom Administrationsagenten an den Administrationsserver übertragen werden sollen. Wenn das Ändern der in diesem Abschnitt angegebenen Einstellungen in der Richtlinie des Administrationsagenten unterbunden ist, können Sie diese Einstellungen nicht ändern. Die Einstellungen im Abschnitt "Datenverwaltung" sind nur auf Geräten verfügbar, die unter Windows laufen:

- Details zu installierten Programmen

  Ist diese Option aktiviert, werden auf den Administrationsserver Informationen über die auf den Client-Geräten installierten Programme 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 auf den Administrationsserver Informationen über Microsoft Windows-Updates übertragen, die auf den Client-Geräten installiert werden sollen.

  Diese Option ist standardmäßig aktiviert. Sie ist nur für Windows verfügbar.

- Informationen über Schwachstellen in Programmen und entsprechende Updates

  Wenn diese Option aktiviert ist, werden Informationen über Schwachstellen in Drittherstellerr-Anwendungen (Microsoft-Software eingeschlossen), die auf verwalteten Geräten erkannt wurden, sowie Informationen über Software-Updates zum Beheben der Drittherstellerr-Schwachstellen (Microsoft-Software 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 von Microsoft-Software 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.

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. Die Einstellungen im Abschnitt **Verwaltung des Neustarts** sind nur auf Geräten verfügbar, die unter Windows laufen:

- **Betriebssystem nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) 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 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. 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. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  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 das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

  Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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, wird ein für den Betrieb des Administrationsagenten erforderlicher UDP-Port zur Liste der Ausschlüsse 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 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. Der standardmäßige UDP-Port für die Verbindung zum KSN-Proxyserver ist 15111.

- **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. Die Einstellungen im Abschnitt **Verbindungsprofile** sind nur auf Geräten verfügbar, die unter Windows laufen:

- **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**

  Verbindungsprofile werden nur für Windows-Geräte unterstützt.

  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 Programme, die auf dem Client-Gerät installiert sind, Richtlinienprofile für Geräte im Modus für mobile Benutzer sowie Richtlinien für mobile Benutzer. 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.

  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:

- **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 das Programm 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 für 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 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. Der standardmäßige UDP-Port für die Verbindung zum KSN-Proxyserver ist 15111.

- **HTTPS über 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 über 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.

- **sudoers-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.

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	✓	✓	✓
Installation mittels Dritthersteller-Tools zur Remote-Installation von Programmen	✓	✓	✓
Installation durch manuelles Starten der Installer der Programme 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	✓	✓	✓
Verteilungspunkt			
Verwendung als Verteilungspunkt	✓	✓	✓
Automatische Zuweisung von Verteilungspunkten	✓	✓ Ohne die Verwendung von Network Location Awareness (NLA).	✓ Ohne die Verwendung Network Location Awa (NLA).
Autonomes Modell für den Download von Updates	✓	✓	✓
Netzwerkabfrage	✓ • IP-Bereiche abfragen • Abfrage des Domänencontrollers	✓ • IP-Bereiche abfragen • Zeroconf-Abfrage • Abfrage des Domänencontrollers (Microsoft Active Directory, Samba 4 Active Directory)	–
KSN Proxy-Service auf dem Verteilungspunkt ausführen	✓	✓	–
Herunterladen von Updates über Kaspersky-Update-Server in die Datenverwaltungen der Verteilungspunkte, welche wiederum die Updates an verwaltete Geräte verteilen	✓	✓	– (Wenn ein oder mehr Geräte, die unter Linux macOS laufen, in den B der Aufgabe zum Dow von Updates in die Datenverwaltung d Verteilungspunkte fa schließt die Aufgabe m Status "Fehlgeschlage selbst wenn sie auf a Windows-Geräten erfolgreich abgeschlo wurde)
Push-Installation von Programmen	✓	Eingeschränkt: Es ist nicht möglich, mithilfe von Linux-Verteilungspunkten eine Push-Installation auf Windows-Geräten durchzuführen.	Eingeschränkt: Es ist möglich, mithilfe von ma Verteilungspunkten e Push-Installation a Windows-Geräten durchzuführen.
Verwendung als Push-Server	✓	✓	–

Umgang mit Anwendungen von Drittanbietern			
Remote-Installation von Programmen auf Geräten	✓	✓	✓
Anpassen von Updates des Betriebssystems in einer Richtlinie des Administrationsagenten	✓	–	–
Informationen über Schwachstellen in Programmen anzeigen	✓	–	–
Schwachstellensuche in Programmen	✓	–	–
Software-Updates	✓	–	–
Inventarisierung von auf Geräten installierten Programmen	✓	✓	–
Virtuelle Maschinen			
Installation des Administrationsagenten auf einer virtuellen Maschine	✓	✓	✓
Einstellungen für Optimierung der Virtual Desktop Infrastructure (VDI)	✓	✓	✓
Unterstützung von dynamischen virtuellen Maschinen	✓	✓	✓
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	✓	✓	✓
Wechsel des Administrationsagenten von einem Administrationsserver auf	✓	–	✓

einen anderen (automatisch nach Netzwerkstandort)			
Verbindung des Client-Geräts mit dem Administrationsserver prüfen. "klnagchk"-Tool	✓	✓	✓
Remotedesktopverbindung mit dem Client-Gerät herstellen	✓	–	✓ Unter Verwendung d Virtual Network Comp Systems (VNC).
Herunterladen eines autonomen Installationspaketes mithilfe des Migrationsassistenten	✓	✓	✓

Vergleich der Einstellungen des Administrationsagenten nach Betriebssystemen

Die folgende Tabelle stellt eine Übersicht über die verfügbaren Einstellungen des Administrationsagenten in Abhängigkeit des Betriebssystems von dem Gerät, auf dem der Administrationsagent installiert ist, dar.

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)** • **Dem Programm ist es erlaubt, auf dem Gerät erweiterte Daten über Richtlinien zu erfassen**	✓
Datenverwaltung	✓	✓ Es sind folgende Optionen verfügbar: • **Details zu installierten Programmen**	✓ Die Option **Informationen über das Hardware-Register** ist verfügbar.

		• **Informationen über die Hardware-Inventur**	
Konnektivität → Netzwerk	✓	✓ Mit Ausnahme der Option **Ports des Administrationsagenten in der Windows-Firewall öffnen**.	✓
Konnektivität → Verbindungsprofile	✓	–	✓
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 Modus für geringen Ressourcenverbrauchs können Sie auf dem Client-Gerät die Auslastung des Arbeitsspeichers durch den installierten Administrationsagenten einschränken. Standardmäßig ist der Modus für geringen Ressourcenverbrauch deaktiviert.

Im Modus für geringen Ressourcenverbrauch 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 der Seite des Verteilungspunkts.
- Hochladen von Updates in die Datenverwaltung des Verteilungspunkts.
- Umgehen der Sperre des DNS-Servers.

Wenn der Modus für geringen Ressourcenverbrauch deaktiviert wird, setzen die Komponenten und Prozesse ihre Ausführung fort.

So aktivieren Sie den Modus für geringen Ressourcenverbrauch:

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 mithilfe des folgenden Befehls, ob der Modus für geringen Ressourcenverbrauch aktiviert ist:

   ```
   $ sudo service klnagent64 status
   ```

   Der Modus für geringem Ressourcenverbrauch wurde aktiviert.

So deaktivieren Sie den Modus für geringen Ressourcenverbrauch:

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
   ```

3. Überprüfen Sie mithilfe des folgenden Befehls, ob der Modus für geringen Ressourcenverbrauch deaktiviert ist:

   ```
   $ sudo service klnagent64 status
   ```

   Der Modus für geringem Ressourcenverbrauch wurde deaktiviert.

Sie können den Modus für geringem Ressourcenverbrauch auch remote aktivieren, indem Sie die Aufgabe *Remote-Ausführung von Skripten* verwenden.

Richtlinie für Kaspersky Endpoint Security manuell konfigurieren

Dieser Abschnitt enthält Empfehlungen zur Konfiguration der Richtlinie von Kaspersky Endpoint Security. Sie können die Einrichtung im Fenster mit den Richtlinieneigenschaften durchführen. Klicken Sie beim Bearbeiten einer Einstellung auf das Schloss-Symbol rechts neben der entsprechenden Gruppe der Einstellungen, um die angegebenen Werte auf eine Workstation anzuwenden.

Kaspersky Security Network konfigurieren

Kaspersky Security Network (KSN) besteht aus einer Infrastruktur aus Cloud-Diensten, die Informationen über die Reputation von Dateien, Webressourcen und Software enthält. Kaspersky Security Network ermöglicht es Kaspersky Endpoint Security für Windows, schneller auf verschiedenste Bedrohungstypen zu reagieren, verbessert die Leistung der Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen. Weitere Informationen zu Kaspersky Security Network finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

So geben Sie die empfohlenen KSN-Einstellungen ein:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie von Kaspersky Endpoint Security für Windows.

   Das Eigenschaftenfenster der gewählten Richtlinie wird geöffnet.
3. Wechseln Sie in den Richtlinieneigenschaften zu **Programmeinstellungen** → **Erweiterter Schutz** → **Kaspersky Security Network**.
4. Stellen Sie sicher, dass die Option **KSN-Proxy verwenden** aktiviert ist. Diese Option unterstützt Sie bei der Umverteilung und Optimierung des Datenverkehrs im Netzwerk.

   Wenn Sie Managed Detection and Response verwenden, müssen Sie die Option **KSN-Proxy** für den Verteilungspunkt und den erweiterten KSN-Modus aktivieren.
5. Aktivieren Sie die Verwendung von KSN-Servern, wenn der KSN Proxy-Service nicht verfügbar ist. KSN-Server können sich sowohl auf der Seite von Kaspersky (wenn KSN verwendet wird) als auch auf der Seite von Dritten (wenn KPSN verwendet wird) befinden.
6. Klicken Sie auf die Schaltfläche **OK**.

Die empfohlenen KSN-Einstellungen werden angegeben.

Liste der durch die Firewall geschützten Netzwerke überprüfen

Stellen Sie sicher, dass die Firewall von Kaspersky Endpoint Security für Windows alle Ihre Netzwerke schützt. Standardmäßig schützt die Firewall Netzwerke mit den folgenden Verbindungstypen:

- **Öffentliches Netzwerk**. Antiviren-Programme, Firewalls oder Filter schützen die Geräte in einem solchen Netzwerk nicht.
- **Lokales Netzwerk**. Der Zugriff auf Dateien und Drucker ist für Geräte in diesem Netzwerk eingeschränkt.
- **Vertrauenswürdiges Netzwerk**. Geräte in einem solchen Netzwerk sind vor Angriffen und unbefugtem Zugriff auf Dateien und Daten geschützt.

Wenn Sie ein benutzerdefiniertes Netzwerk konfiguriert haben, stellen Sie sicher, dass es durch die Firewall geschützt wird. Überprüfen Sie dazu die Liste der Netzwerke in den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows. In der Liste werden möglicherweise nicht alle Netzwerke angezeigt.

Weitere Informationen zur Firewall finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

Um die Liste der Netzwerke zu überprüfen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie von Kaspersky Endpoint Security für Windows.
   Das Eigenschaftenfenster der gewählten Richtlinie wird geöffnet.
3. Wechseln Sie in den Richtlinieneigenschaften zu **Programmeinstellungen** → **Basisschutz** → **Firewall**.
4. Klicken Sie unter **Verfügbare Netzwerke** auf den Link **Netzwerkeinstellungen**.
   Das Fenster **Netzwerkverbindungen** wird geöffnet. In diesem Fenster wird die Liste der Netzwerke angezeigt.
5. Wenn die Liste ein fehlendes Netzwerk enthält, fügen Sie es hinzu.

Untersuchung von Netzwerkgeräten deaktivieren

Die Untersuchung von Netzlaufwerken durch Kaspersky Endpoint Security für Windows kann diese stark belasten. Daher ist es zweckmäßiger, die Untersuchung unmittelbar auf den Dateiservern auszuführen.

Sie können das Untersuchen von Netzlaufwerken in den Richtlinieneigenschaften von Kaspersky Endpoint Security für Windows deaktivieren. Eine Beschreibung dieser Einstellungen finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

Um die Untersuchung von Netzlaufwerken zu deaktivieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie von Kaspersky Endpoint Security für Windows.
   Das Eigenschaftenfenster der gewählten Richtlinie wird geöffnet.
3. Wechseln Sie in den Richtlinieneigenschaften zu **Programmeinstellungen** → **Basisschutz** → **Schutz vor bedrohlichen Dateien**.
4. Deaktivieren Sie unter **Schutzbereich** die Option **Alle Netzlaufwerke**.
5. Klicken Sie auf die Schaltfläche **OK**.

Das Scannen von Netzlaufwerken ist deaktiviert.

Programminformationen aus dem Speicher des Administrationsservers ausschließen

Es wird empfohlen, dass der Administrationsserver keine Informationen über Programm-Module speichert, die auf den Netzwerkgeräten gestartet wurden. Dadurch wird der Speicher des Administrationsservers nicht überlastet.

Sie können das Speichern dieser Information in der Richtlinie von Kaspersky Endpoint Security für Windows deaktivieren.

Um das Speichern von Informationen über installierte Programm-Module zu deaktivieren:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie von Kaspersky Endpoint Security für Windows.

   Das Eigenschaftenfenster der gewählten Richtlinie wird geöffnet.
3. Wechseln Sie in den Richtlinieneigenschaften zu **Programmeinstellungen** → **Allgemeine Einstellungen** → **Berichte und Speicher**.
4. Deaktivieren Sie das Kontrollkästchen **Über die ausgeführten Programme**, unter **Datenübertragung an den Administrationsserver**, wenn diese in der übergeordneten Richtlinie noch aktiviert ist.

   Wenn dieses Kontrollkästchen aktiviert ist, werden in der Datenbank des Administrationsservers 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.

Informationen über installierte Programm-Module werden nicht länger in der Datenbank des Administrationsservers gespeichert.

Zugriff auf die Benutzeroberfläche von Kaspersky Endpoint Security für Windows für Workstations konfigurieren

Wenn der Virenschutz im Unternehmensnetzwerk zentral über Kaspersky Security Center Linux verwaltet werden muss, geben Sie die Schnittstelleneinstellungen in den Richtlinieneigenschaften von Kaspersky Endpoint Security für Windows wie unten beschrieben an. Dadurch verhindern Sie den unbefugten Zugriff auf Kaspersky Endpoint Security für Windows auf Workstations und die Änderung der Einstellungen von Kaspersky Endpoint Security für Windows.

Eine Beschreibung dieser Einstellungen finden Sie in der Hilfe zu Kaspersky Endpoint Security für Windows.

Um die empfohlenen Einstellungen der Benutzerschnittstelle anzugeben:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie von Kaspersky Endpoint Security für Windows.

   Das Eigenschaftenfenster der gewählten Richtlinie wird geöffnet.
3. Wechseln Sie in den Richtlinieneigenschaften zu **Programmeinstellungen** → **Allgemeine Einstellungen** → **Benutzeroberfläche**.
4. Wählen Sie unter **Interaktion mit dem Benutzer** die Option **Keine Benutzerschnittstelle**. Dadurch wird die Anzeige der Benutzeroberfläche von Kaspersky Endpoint Security für Windows auf Workstations deaktiviert, sodass deren Benutzer die Einstellungen von Kaspersky Endpoint Security für Windows nicht ändern können.
5. Aktivieren Sie unter **Kennwortschutz** die Umschaltfläche. Dies reduziert das Risiko unautorisierter oder unabsichtlicher Änderungen in dem Einstellungen von Kaspersky Endpoint Security für Windows auf Workstations.

Die empfohlenen Einstellungen der Benutzerschnittstelle von Kaspersky Endpoint Security für Windows sind angegeben.

Wichtige Ereignisse von Richtlinien in der Datenbank des Administrationsservers speichern

Um einen Überlauf der Datenbank des Administrationsservers zu vermeiden, empfehlen wir Ihnen, nur wichtige Ereignisse in der Datenbank zu speichern.

So konfigurieren Sie die Registrierung wichtiger Ereignisse in der Datenbank des Administrationsservers:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie von Kaspersky Endpoint Security für Windows.

   Das Eigenschaftenfenster der gewählten Richtlinie wird geöffnet.
3. Wechseln Sie in den Eigenschaften für Richtlinien zur Registerkarte **Konfiguration von Ereignissen**.
4. Klicken Sie im Abschnitt **Kritisch** auf **Ereignis hinzufügen** und aktivieren Sie die Kontrollkästchen neben den folgenden Ereignissen:
   - *Verletzung des Endbenutzer-Lizenzvertrags*
   - *Autostart des Programms ist deaktiviert*
   - *Aktivierungsfehler*
   - *Aktive Bedrohung gefunden. Erweiterte Desinfektion sollte ausgeführt werden*
   - *Desinfektion nicht möglich*
   - *Früher geöffneter gefährlicher Link gefunden*
   - *Prozess beendet*
   - *Netzwerkaktivität verboten*
   - *Netzwerkangriff gefunden*
   - *Anwendungsstart verboten*
   - *Zugriff verweigert (Lokale Datenbanken)*
   - *Zugriff verweigert (KSN)*
   - *Lokaler Update-Fehler*
   - *Der Start von zwei Aufgaben gleichzeitig ist unmöglich*
   - *Fehler bei der Interaktion mit Kaspersky Security Center*
   - *Nicht alle Komponenten aktualisiert*
   - *Fehler beim Übernehmen der Verschlüsselungs- bzw. Entschlüsselungsregeln der Dateien*

- *Fehler bei der Aktivierung des portablen Modus*
- *Fehler bei der Deaktivierung des portablen Modus*
- *Das Verschlüsselungsmodul konnte nicht geladen werden*
- *Richtlinie kann nicht übernommen werden*
- *Fehler beim Ändern der Programmkomponenten*

5. Klicken Sie auf die Schaltfläche **OK**.
6. Klicken Sie im Abschnitt **Funktionsfehler** auf **Ereignis hinzufügen** und aktivieren Sie ausschließlich das Kontrollkästchen neben dem Ereignis *Ungültige Aufgabeneinstellungen. Aufgabeneinstellungen nicht übernommen*.
7. Klicken Sie auf die Schaltfläche **OK**.
8. Klicken Sie im Abschnitt **Warnung** auf **Ereignis hinzufügen** und aktivieren Sie die Kontrollkästchen neben den folgenden Ereignissen:
   - *Selbstschutz des Programms wurde deaktiviert*
   - *Schutzkomponenten sind deaktiviert*
   - *Reserveschlüssel ist ungültig*
   - *Legitime Software, die von Eindringlingen zur Beeinträchtigung Ihres Computers bzw. Ihrer persönlichen Daten missbraucht werden kann, wurde gefunden (lokale Datenbanken)*
   - *Legitime Software, die von Eindringlingen zur Beeinträchtigung Ihres Computers bzw. Ihrer persönlichen Daten missbraucht werden kann, wurde gefunden (KSN)*
   - *Objekt gelöscht*
   - *Objekt desinfiziert*
   - *Der Benutzer hat die Verschlüsselungsrichtlinie abgelehnt*
   - *Die Datei wurde vom Administrator aus der Quarantäne auf dem Server von Kaspersky Anti Targeted Attack Platform wiederhergestellt*
   - *Die Datei wurde vom Administrator auf dem Server von Kaspersky Anti Targeted Attack Platform in die Quarantäne verschoben*
   - *Nachricht beim Verbot des Anwendungsstarts an den Administrator*
   - *Nachricht beim Verbot des Zugriffs auf das Gerät an den Administrator*
   - *Nachricht beim Verbot des Zugriffes auf eine Webseite an den Administrator*
9. Klicken Sie auf die Schaltfläche **OK**.
10. Klicken Sie im Abschnitt **Information** auf **Ereignis hinzufügen** und aktivieren Sie die Kontrollkästchen neben den folgenden Ereignissen:

- *Eine Backup-Kopie des Objekts wurde erstellt*
- *Der Start der Anwendung ist im Testbetrieb untersagt*

11. Klicken Sie auf die Schaltfläche **OK**.

Die Registrierung wichtiger Ereignisse in der Datenbank des Administrationsservers ist konfiguriert.

Gruppenaufgabe zum Aktualisieren von Kaspersky Endpoint Security manuell konfigurieren

Der optimale und empfohlene Zeitplan für Kaspersky Endpoint Security ist **Nach dem Download von Updates in die Datenverwaltung**, wenn das Kontrollkästchen **Automatische zufällige Verzögerung für Aufgabenstarts verwenden** aktiviert ist.

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.

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 Programme 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-Programme, 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-Programme, 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-Programmen ermöglicht, Zugriff auf die Reputationsdatenbanken von Kaspersky Security Network und andere statistische Daten zu erhalten, ohne Daten von ihren eigenen Computern an 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-Einstellungen** 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 oder einer Aktualisierung 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 das Programm 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 und an KSN Informationen 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-Einstellungen** 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN Proxy-Einstellungen** aus.

3. Stellen Sie den Umschalter auf die Position **KSN Proxy auf dem Administrationsserver aktivieren Aktiviert**.

Die Übertragung von Daten der Client-Geräte an KSN wird durch die Richtlinie von Kaspersky Endpoint Security geregelt, die auf den Client-Geräten in Kraft ist. Wenn das Kontrollkästchen deaktiviert ist, findet keine Übertragung von Daten des Administrationsservers bzw. der Client-Geräte über Kaspersky Security Center Linux an KSN statt. 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. Stellen Sie den Umschalter auf die Position **Kaspersky Security Network verwenden Aktiviert**.

   Wenn diese Option aktiviert ist, senden Client-Geräte die Ergebnisse der Patch-Installation an Kaspersky. 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 auswählen**, 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-Programme 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-Einstellungen** 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 über 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-Einstellungen** 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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.

KSN aktivieren und deaktivieren

Um KSN zu aktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN Proxy-Einstellungen** aus.

3. Stellen Sie den Umschalter auf die Position **KSN Proxy auf dem Administrationsserver aktivieren Aktiviert**.

   Der Dienst des KSN-Proxyservers wird aktiviert.

4. Stellen Sie den Umschalter auf die Position **Kaspersky Security Network verwenden Aktiviert**.

   Daraufhin wird KSN aktiviert.

   Wenn dieser Umschalter aktiviert ist, senden Client-Geräte die Ergebnisse der Patch-Installation an Kaspersky. Wenn Sie den Umschalter aktivieren, müssen Sie die Bestimmungen der KSN-Erklärung lesen und akzeptieren.

5. Klicken Sie auf die Schaltfläche **Speichern**.

Um die KSN zu deaktivieren, gehen Sie wie folgt vor:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN Proxy-Einstellungen** aus.

3. Stellen Sie den Umschalter auf die Position **KSN Proxy auf dem Administrationsserver aktivieren Deaktiviert**, um den KSN Proxy-Service zu deaktivieren, oder stellen Sie den Umschalter auf die Position **Kaspersky Security Network verwenden Deaktiviert**.

   Wenn einer der Umschalter deaktiviert ist, werden von den Client-Geräten keine Ergebnisse über die Installation von Patches an Kaspersky übermittelt.

   Wenn Sie KPSN verwenden, setzen Sie den Umschalter auf die Position **Kaspersky Private Security Network verwenden Deaktiviert**.

   Daraufhin wird KSN deaktiviert.

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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **KSN Proxy-Einstellungen** 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 oder einer Aktualisierung des Administrationsservers angezeigt. Sie können die aktualisierte KSN-Erklärung akzeptieren oder ablehnen. Wenn Sie diese ablehnen, werden Sie KSN weiterhin gemäß der Version der KSN-Erklärung verwenden, die Sie zuvor akzeptiert haben.

Nach einem Update oder einem Upgrade des Administrationsservers wird die aktualisierte KSN-Erklärung automatisch angezeigt. Wenn Sie die aktualisierte KSN-Erklärung ablehnen, können Sie diese später erneut anzeigen und akzeptieren.

Um die KSN-Erklärung anzuzeigen und anschließend zu akzeptieren:

1. Klicken Sie auf den Link **Benachrichtigungen anzeigen** in der oberen rechten Ecke des Hauptanwendungsfensters.

   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 entscheiden Sie sich anschließend durch Anklicken einer 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 in den Eigenschaften des Administrationsservers jederzeit 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. Zeigen Sie auf dem Gerät, dass als Verteilungspunkt fungiert, die Liste der ausgeführten Prozesse an.

2. Überprüfen Sie, ob in der Liste der laufenden Prozesse, der Prozess `/opt/kaspersky/ksc64/sbin/ksnproxy` läuft.

Wenn der Dienst `opt/kaspersky/ksc64/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.

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 Programmen, Untersuchung von Dateien, Datenbanken-Update und Aktualisierung der Programm-Module sowie Ausführung anderer Aktionen mit den Programmen.

Aufgaben für ein bestimmtes Programm können mithilfe von Kaspersky Security Center Web Console nur dann erstellt werden, wenn das Verwaltungs-Plug-in für dieses Programm auf dem der Server der Kaspersky Security Center Web Console 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 Sicherheits-App). 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 jedes Programm 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 das Programm gestartet wurde, für das diese Aufgaben erstellt worden waren.

Ausführungsergebnisse von Aufgaben werden im Betriebssystem-Ereignisprotokolle auf jedem Gerät, im Betriebssystem-Ereignisprotokoll des Administrationsservers und in der Datenbank des Administrationsservers 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 der Satz 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.

- 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 Datenbank des Administrationsservers eingegeben wurden. Darüber hinaus müssen die Informationen entweder während einer bestehenden Verbindung der Geräte oder während einer Gerätesuche eingegeben worden sein.

- Geräteauswahl festlegen.

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 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 **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **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.

So erstellen Sie eine neue Aufgabe, die ausgewählten Geräten zugewiesen wird:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete 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 **Verwaltete 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 **Assets (Geräte)** → **Aufgaben**.
2. Aktivieren Sie in der Aufgabenliste das Kontrollkästchen neben der Aufgabe, die Sie starten möchten.
3. Klicken Sie auf die Schaltfläche **Starten**.

   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 sie 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 **Assets (Geräte)** → **Verwaltete Geräte**. Die Liste der verwalteten Geräte wird angezeigt.

Wählen Sie in der Liste der verwalteten Geräte die Geräte, für die Sie die Aufgabe ausführen möchten, mithilfe der Kontrollkästchen aus. Sie können die Such- und Filterfunktionen verwenden, um die gewünschten Geräte zu finden.

1. Klicken Sie auf die Schaltfläche **Aufgabe ausführen** und wählen Sie anschließend **Bestehende Aufgabe anwenden** aus.

   Die Liste der vorhandenen Aufgaben wird angezeigt.
2. Die ausgewählten Geräte werden oberhalb der Aufgabenliste angezeigt. Bei Bedarf können Sie Geräte aus dieser Liste entfernen. Die Liste muss mindestens ein Gerät enthalten.
3. Wählen Sie die gewünschte Aufgabe aus der Liste aus. Sie können das Suchfeld oberhalb der Liste verwenden, um die gewünschte Aufgabe anhand ihres Namens zu finden. Es kann nur eine Aufgabe ausgewählt werden.
4. Klicken Sie auf **Aufgabe speichern und ausführen**.

   Die ausgewählte Aufgabe wird für die ausgewählten Geräte sofort gestartet. Der konfigurierte Zeitplan 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 **Assets (Geräte)** → **Aufgaben**.

Die Aufgabenliste wird angezeigt. Die Aufgaben sind nach den Namen der Programme gruppiert, auf die sie sich beziehen. Beispielsweise bezieht sich die Aufgabe *Remote-Installation eines Programms* 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. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) 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 Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

  - **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- Beenden von Anwendungen in blockierten Sitzungen erzwingen

  Laufende Anwendungen können das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

  Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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:
  - **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 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.

    - 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.

    - Täglich (Sommerzeit wird nicht unterstützt)

Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Abwärtskompatibilität von Kaspersky Security Center Linux benötigt.

Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Wöchentlich**

  Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit 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.

- **Monatlich, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig sind keine Tage des Monats ausgewählt. Die Standardstartzeit beträgt 18:00 Uhr.

- **Nach dem Download von 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 Beenden 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 des Programms von Kaspersky 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.

    Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Vielleicht wollen 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 Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen festlegen.

    Sie können diese Option beispielsweise verwenden, um eine Aufgabe auf Geräten mit einer bestimmten Betriebssystemversion auszuführen.

  - **Aufgabe einer Administrationsgruppe zuweisen**

    Die Aufgabe wird Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen festlegen oder eine neue erstellen.

    Sie können diese Option beispielsweise zum Starten einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die in einer bestimmten Administrationsgruppe enthalten sind.

- Benutzerkonto-Einstellungen:
  - **Standardbenutzerkonto**

    Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, unter dem das Programm installiert und gestartet wurde, dass diese Aufgabe ausführt.

    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 dessen Namen 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 anhalten, 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

      Programmereignisse, 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

Programmereignisse, 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 **Assets (Geräte)** → **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.

Um eine Aufgabe zu importieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **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 Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen festlegen oder eine neue erstellen.

     Sie können diese Option beispielsweise zum Starten einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die in einer bestimmten Administrationsgruppe enthalten sind.

   - 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.

     Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Vielleicht wollen 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 Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen festlegen.

     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 erfolgreichem Import wird die Aufgabe in der Liste der Aufgaben angezeigt. Die Einstellungen und der Zeitplan der Aufgabe werden ebenfalls importiert. Die Aufgabe wird gemäß ihres Zeitplans 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 **Assets (Geräte)** → **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 beschreibt die Programm-Tags und bietet eine Anleitung für deren Erstellung und Änderung sowie für das Zuweisen von Tags an Drittanbieter-Apps.

Über Programm-Tags

Mit Kaspersky Security Center Linux können Sie den Anwendungen in der Programm-Registry Tags hinzufügen. Ein Tag ist eine Bezeichnung, anhand derer Programme gruppiert und gefunden werden können. Einem Programm zugewiesene Tags können als Bedingung in 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 Programm-Tag zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-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 Programm-Tags angezeigt.

Programm-Tag umbenennen

Um ein Programm-Tag umzubenennen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-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 Programm-Tags angezeigt.

Einem Programm Tags zuweisen

Um einem Programm ein oder mehrere Tags zuzuweisen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.
2. Klicken Sie auf den Namen des Programms, dem Sie Tags zuweisen möchten.
3. Wählen Sie die Registerkarte **Tags** aus.

   Die Registerkarte zeigt alle Programm-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. 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 dem Programm zugewiesen.

Zugewiesene Tags von einem Programm entfernen

Um ein oder mehrere Tags von einem Programm zu entfernen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.
2. Klicken Sie auf den Namen des Programms, von dem Sie Tags entfernen möchten.
3. Wählen Sie die Registerkarte **Tags** aus.

   Die Registerkarte zeigt alle Programm-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 vom Programm entfernt.

Die entfernten Tags werden nicht gelöscht. Bei Bedarf können Sie diese manuell löschen.

Programm-Tag löschen

Um ein Programm-Tag zu löschen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Tags**.
2. Wählen Sie in der Liste das Programm-Tag aus, das Sie löschen möchten.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **OK**.

Das Programm-Tag wird gelöscht. Das gelöschte Tag wird automatisch von allen Programmen entfernt, denen es zugewiesen war.

Offline-Zugriff auf ein externes Gerät gewähren, das von der Gerätekontrolle blockiert wurde

In der Komponente "Gerätekontrolle" der Richtlinie von Kaspersky Endpoint Security können Sie den Benutzerzugriff auf externe Geräte verwalten, die auf dem Client-Gerät (z. B. Festplatten, Kameras oder WLAN-Module) installiert oder mit diesem verbunden sind. Dadurch können Sie das Client-Gerät vor Infektionen schützen, wenn solche externen Geräte verbunden werden, und so einen Datenverlust oder Datenlecks verhindern.

Wenn Sie temporären Zugriff auf ein externes Gerät gewähren möchten, das von der "Gerätekontrolle" blockiert wurde, dieses Gerät jedoch nicht zur Liste der vertrauenswürdigen Geräte hinzugefügt werden kann, so können Sie vorübergehend Offline-Zugriff auf das externe Gerät gewähren. Offline-Zugriff bedeutet, dass das Client-Gerät keinen Zugriff auf das Netzwerk hat.

Sie können dem durch die Gerätesteuerung blockierten externen Gerät nur Offline-Zugriff gewähren, wenn die Option **Anfrage auf temporären Zugriff erlauben** in den Einstellungen der Richtlinie von Kaspersky Endpoint Security im Abschnitt **Programmeinstellungen** → **Sicherheitskontrollen** → **Gerätesteuerung** aktiviert ist.

Die Gewährung des Offline-Zugriffs auf ein externes Gerät, das von der "Gerätekontrolle" blockiert wurde, umfasst die folgenden Schritte:

1. Der Gerätebenutzer, der Zugriff auf das blockierte externe Gerät wünscht, generiert im Dialogfenster von Kaspersky Endpoint Security eine Zugriffsanfrage-Datei und sendet diese Datei an den Administrator für Kaspersky Security Center Linux.
2. Wenn der Administrator für Kaspersky Security Center Linux diese Anfrage erhält, erstellt er eine Zugriffsschlüssel-Datei und sendet diese Datei an den Gerätebenutzer.
3. Der Benutzer aktiviert die Zugriffsschlüssel-Datei im Dialogfenster von Kaspersky Endpoint Security und erhält temporären Zugriff auf das externe Gerät.

Um temporären Zugriff auf ein externes Gerät zu gewähren, das von der "Gerätekontrolle" blockiert wurde:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.

   Die Liste der verwalteten Geräte wird angezeigt.

2. Wählen Sie in dieser Liste das Benutzergerät aus, das um Zugriff auf das externe Gerät bittet, das von der "Gerätekontrolle" blockiert wurde.

   Sie können nur ein Gerät auswählen.

3. Klicken Sie oberhalb der Liste auf die Ellipse-Schaltfläche (...) und klicken Sie anschließend auf die Schaltfläche **Zugriff auf das Gerät im autonomen Modus gewähren**.

4. Klicken Sie im angezeigten Fenster **Programmeinstellungen** im Abschnitt **Gerätekontrolle** auf die Schaltfläche **Durchsuchen**.

5. Wählen Sie die Zugriffsanforderungsdatei aus, die Sie vom Benutzer erhalten haben, und klicken Sie anschließend auf die Schaltfläche **Öffnen**. Die Datei sollte das akey-Format besitzen.

   Es werden Details über das gesperrte Gerät angezeigt, auf das der Benutzer den Zugriff erbittet.

6. Geben Sie einen Wert für die **Zugriffsdauer** an.

   Diese Einstellung gibt an, wie lange Sie dem Benutzer Zugriff auf das gesperrte Gerät gewähren. Der Standardwert ist der Wert, den der Benutzer beim Erstellen der Zugriffsanfrage-Datei angegeben hat.

7. Geben Sie einen Wert für die **Aktivierungsfrist** an.

   Diese Einstellung gibt den Zeitraum an, im dem der Benutzer den Zugriff auf das gesperrte Gerät mithilfe des bereitgestellten Zugriffsschlüssels aktivieren kann.

8. Klicken Sie auf die Schaltfläche **Speichern**.

9. Wählen Sie im geöffneten Fenster den Zielordner aus, in dem Sie die Datei speichern möchten, die den Zugriffsschlüssel für das blockierte Gerät enthält.

10. Klicken Sie auf die Schaltfläche **Speichern**.

Nachdem Sie die Zugriffsschlüssel-Datei an den Benutzer gesendet haben und der Benutzer die Datei in Kaspersky Endpoint Security aktiviert hat, erhält der Benutzer für den festgelegten Zeitraum temporären Zugriff auf das blockierte Gerät.

Verwendung des klscflag-Dienstprogramms, um Port 13291 zu öffnen

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` bedeutet, dass der Port geöffnet ist. Andernfalls wird der Wert `false` angezeigt.

Die Web-Oberfläche von 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 Web Console von Kaspersky Security Center 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 Synchronisation des Servers von Kaspersky Industrial CyberSecurity for Networks mit dem Administrationsserver warten. Nachdem das Plug-in heruntergeladen und installiert wurde, wird der Abschnitt **KICS for Networks** im Hauptmenü der Kaspersky Security Center Web Console angezeigt.

   - In der Benutzeroberfläche von Kaspersky Industrial CyberSecurity for Networks wird 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 **Entdeckung und Bereitstellung** → **Nicht zugeordnete 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 Fenster mit den Eigenschaften 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 die Schaltfläche **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.

   Das 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. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.

   b. Klicken Sie im Dashboard auf die Schaltfläche **Widget hinzufügen oder wiederherstellen**.

   c. Wählen Sie im sich öffnenden Widget-Menü die Option **Andere**.

   d. Wählen Sie das Widget aus, das Sie hinzufügen möchten.

      - Bereitstellungs-Übersicht 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. So wechseln Sie zur Web-Oberfläche von Kaspersky Industrial CyberSecurity for Networks:

   a. Wechseln 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 aus der Dropdown-Liste mit Servern, die mit Kaspersky Security Center integriert sind, "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 Weboberfläche 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 zwei Typen von Benutzerkonten:

- Benutzerkonten der Mitarbeiter einer Organisation. Der Administrationsserver erhält Daten über die Konten dieser lokalen Benutzer beim Abfragen des Unternehmensnetzwerks.
- Benutzerkonten für interne Benutzer von Kaspersky Security Center Linux. Auf dem Portal können Sie Konten für interne Benutzer erstellen. Diese Benutzerkonten werden nur innerhalb von Kaspersky Security Center Linux verwendet.

So zeigen Sie Tabellen mit Benutzerkonten und Sicherheitsgruppen an:

1. Wechseln 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 **Untertyp** auf **Intern** bzw. **Lokal**.

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 Anwendung von Kaspersky 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 bietet Unterstützungen für eine rollenbasierte Zugriffskontrolle auf die Funktionen von Kaspersky Security Center Linux und von verwalteten Kaspersky-Programmen an.

Sie können die Zugriffsrechte auf Programmfunktionen 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 entsprechend ihrer dienstlichen Verpflichtungen.

Die Verwendung von Benutzerrollen soll die stets wiederkehrenden Abläufe für das Konfigurieren von Zugriffsrechten der Benutzer auf Programmfunktionen vereinfachen und verkürzen. Die Zugriffsberechtigungen werden in der Rolle entsprechend der typischen Aufgaben und dienstlichen Verpflichtungen des Benutzers festgelegt.

Die Benutzerrollen können einen ihrem Verwendungszweck entsprechenden Namen erhalten. Es kann eine unbegrenzte Anzahl von Rollen erstellt werden.

Sie können entweder vorkonfigurierte Benutzerrollen mit bereits festgelegten Zugriffsrechten verwenden oder neue Rollen erstellen und die notwendigen Berechtigungen selbst konfigurieren.

Zugriffsrechte auf Programmfunktionen

Die unten stehende Tabelle gibt die Funktionen von Kaspersky Security Center Linux mit den Zugriffsrechten für die Verwaltung der damit verknüpften Aufgaben, Berichte und Einstellungen, sowie für das Durchführen der damit verknüpften Benutzervorgänge an.

Um einen in der Tabelle aufgeführten Vorgang auszuführen, muss ein 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.

Der Funktionsbereich **Allgemeine Funktionen**: **Zugriff auf Objekte, unabhängig von deren ACLs** ist für Audit-Zwecke vorgesehen. Wenn die Benutzer die Berechtigung **Lesen** für diesen Funktionsbereich besitzen, erhalten sie vollständigen **Lesezugriff** auf alle Objekte und können alle erstellten Aufgaben auf ausgewählten Geräten ausführen, die mit lokalen Administratorrechten (root für Linux) über den Administrationsagenten mit dem Administrationsserver verbunden sind. Es wird empfohlen, diese Rechte umsichtig zu gewähren und nur einer begrenzten Anzahl von Benutzern zu zuzuweisen, die diese Rechte zur Erfüllung ihrer offiziellen Aufgaben benötigen.

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
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**	Nichts
Allgemeine Funktionen: **Zugriff auf Objekte, unabhängig von ihren ACLs**	**Lesen**	Lesenden Zugriff auf alle Objekte bekommen: **Lesen**	Nichts

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**	• "Download von U in die Datenverw des Administrationss • "Berichte sende • "Installationspak verteilen" • "Remote-Installa eines Programm sekundären Administrationss

Allgemeine Funktionen: **Gelöschte Objekte**	• **Lesen** • **Schreiben**	• Gelöschte Objekte im Papierkorb anzeigen: **Lesen** • Objekte aus dem Papierkorb löschen: **Schreiben**	Nichts
Allgemeine Funktionen: **Verarbeitung von Ereignissen**	• **Ereignisse löschen** • **Einstellungen der Ereignisbenachrichtigung bearbeiten**	• Einstellungen der Ereignisregistrierung ändern: **Einstellungen der Ereignisprotokollierung bearbeiten**	Nichts

	• **Einstellungen der Ereignisprotokollierung bearbeiten** • **Schreiben**	• Einstellungen der Ereignisbenachrichtigung ändern: **Einstellungen der Ereignisbenachrichtigung bearbeiten** • Ereignisse löschen: **Ereignisse löschen**	
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 Datenbank des Administrationsservers gespeichert sind, angeben: **Schreiben**	• "Backup der Dat Administrationss anlegen" • "Pflege von Datenbanken"

		• Maximale Anzahl von Ereignissen, die der Administrationsserver versenden kann, angeben: **Schreiben** • Zeitspanne, in welcher Ereignisse durch den Administrationsserver versendet werden können, angeben: **Schreiben**	
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
Allgemeine Funktionen: **Schlüsselverwaltung**	• **Schlüsseldatei exportieren** • **Schreiben**	• Schlüsseldatei exportieren: **Schlüsseldatei exportieren** • Einstellungen des Lizenzschlüssels des Administrationsservers ändern: **Schreiben**	Nichts
Allgemeine Funktionen: **Erzwungene Berichtsverwaltung**	• **Lesen** • **Schreiben**	• Berichte unabhängig von ihren ACLs erstellen: **Schreiben** • Berichte unabhängig von ihren ACLs exportieren: **Lesen**	Nichts
Allgemeine Funktionen: **Hierarchie von**	**Hierarchie von Administrationsservern**	• Sekundäre Administrationsserver	Nichts

Administrationsservern	**konfigurieren**	registrieren, aktualisieren oder löschen: **Hierarchie von Administrationsservern konfigurieren**	
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
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
Allgemeine Funktionen:	**Schreiben**	Importieren von	Nichts

Verwaltung der Chiffrierschlüssel		Chiffrierschlüsseln: **Schreiben**	
Systemverwaltung: **Schwachstellen- und Patch-Management**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	• Eigenschaften von Patches von Drittherstellern anzeigen: **Lesen** • Eigenschaften von Patches von Drittherstellern ändern: **Schreiben**	• "Schwachsteller schließen" • "Erforderliche U installieren und Schwachstellen schließen"
Systemverwaltung: **Remote-Ausführung von Skripten**	• **Lesen** • **Schreiben** • **Ausführen** • **Vorgänge auf Geräteauswahlen ausführen**	Der Benutzer kann die Aufgabeneigenschaften anzeigen: **Lesen** Der Benutzer kann ein Installationspaket erstellen, löschen oder ändern: **Schreiben** 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**	"Remote-Ausführur Skripten"

Vorkonfigurierte Benutzerrollen

Benutzer von Kaspersky Security Center Linux mit zugewiesenen Benutzerrollen bekommen Zugriffsrechte auf Programmfunktionen gewährt.

Benutzern, die auf einem virtuellen Server erstellt wurden, können auf dem Administrationsserver keine Rollen zugewiesen werden.

Sie können entweder vorkonfigurierte Benutzerrollen mit bereits festgelegten Zugriffsrechten verwenden oder neue Rollen erstellen und die notwendigen Berechtigungen selbst konfigurieren. 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 Vorgänge mit allen Berichtstypen, alle Anzeige-Vorgänge, einschließlich der Anzeige gelöschter Objekte (gewährt die Berechtigungen **Lesen** und **Schreiben** im Bereich **Gelöschte Objekte**). Erlaubt keine anderen Vorgänge. Sie können diese Rolle einer Person zuweisen, die das Audit Ihres Unternehmens durchführt.
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.

Die Funktionen der Funktionsbereiche **Verwaltung mobiler Geräte: Allgemein** und **Systemverwaltung** sind in Kaspersky Security Center Linux nicht verfügbar.

Zugriffsberechtigungen von vorkonfigurierten Benutzerrollen

Rolle	Beschreibung
Administrator des Administrationsserver	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen in **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Verarbeitung von Ereignissen** • **Hierarchie des Administrationsservers** • **Virtuelle Administrationsserver** Gewährt die Berechtigungen **Lesen** und **Schreiben** in dem Funktionsbereich **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel**.
Operator des Administrationsserver	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen innerhalb von **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Virtuelle Administrationsserver**
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 in **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Kaspersky software deployment** • **Verwaltung von Lizenzschlüsseln** Gewährt die Berechtigungen **Lesen** und **Ausführen** in dem Funktionsbereich **Allgemeine Funktionen: Virtuelle Administrationsserver**.

Installationsoperator	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen innerhalb von **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Kaspersky Bereitstellung** (gewährt auch die Berechtigung **Verwaltung von Kaspersky Lab-Patches** in diesem Bereich) • **Virtuelle Administrationsserver**
Administrator von Kaspersky Endpoint Security	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • Alle Funktionen aus dem Bereich von Kaspersky Endpoint Security Gewährt die Berechtigungen **Lesen** und **Schreiben** in dem Funktionsbereich **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel**.
Operator von Kaspersky Endpoint Security	Gewährt die Berechtigungen **Lesen** und **Ausführen** in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen: Grundlegende Funktionen** • 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** Gewährt die Berechtigungen **Lesen** und **Schreiben** in dem Funktionsbereich **Allgemeine Funktionen: Verwaltung der Chiffrierschlüssel**.
Hauptoperator	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in allen folgenden Funktionsbereichen: • **Allgemeine Funktionen**: • **Grundlegende Funktionen** • **Gelöschte Objekte** • **Vorgänge auf dem Administrationsserver** • **Bereitstellung der Software von Kaspersky Lab** • **Virtuelle Administrationsserver** • Alle Funktionen aus dem Bereich von Kaspersky Endpoint Security
Administrator der Funktion "Verwaltung mobiler Geräte"	Erlaubt alle Operationen im Funktionsbereich **Allgemeine Funktionen: Basisfunktionen**.
Security Officer	Erlaubt alle Vorgänge in den folgenden Funktionsbereichen in **Allgemeine Funktionen**:

	• **Zugriff auf Objekte, unabhängig von deren ACLs** • **Erzwungene Berichtsverwaltung** Gewährt die Berechtigungen **Lesen**, **Schreiben**, **Ausführen**, **Dateien von Geräten auf dem Administrator-Arbeitsplatz speichern** und **Ausführen von Vorgängen für die Geräteauswahlen** im Funktionsbereich **Systemverwaltung: Verbindungen**. 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**. Diese Funktionen wird nur von Kaspersky Security Center 11 oder höher unterstützt.
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 Funktionen** und **Systemverwaltung** (einschließlich aller Funktionen).
Operator der Funktionen "Schwachstellen- und Patch-Management"	Gewährt die Berechtigungen **Lesen** und **Ausführen** (falls anwendbar) in den Funktionsbereichen **Allgemeine Funktionen**: **Grundlegende Funktionen** und **Systemverwaltung** (einschließlich aller Funktionen).

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. Wechseln Sie je nach Objekttyp im Hauptmenü zum entsprechenden Abschnitt:
   - **Assets (Geräte) → Gruppenhierarchie**
   - **Assets (Geräte) → Aufgaben**
   - **Überwachung und Berichterstattung → Berichte**

- **Assets (Geräte) → Geräteauswahlen**
- **Überwachung und Berichterstattung → 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. Wechseln 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.

Benutzern und Gruppen Zugriffsrechte zuweisen

Sie können Benutzern und Gruppen Zugriffsrechte zur Nutzung verschiedener Funktionen des Administrationsservers und der Kaspersky-Programme, für die Sie über Verwaltungs-Plug-ins verfügen, erteilen, beispielsweise Kaspersky Endpoint Security für Linux.

So weisen Sie einem Benutzer oder einer Benutzergruppe Zugriffsrechte zu:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Aktivieren Sie auf der Registerkarte **Zugriffsrechte** das Kontrollkästchen neben dem Namen des Benutzers oder der Sicherheitsgruppe, dem oder der Sie die Rechte zuweisen möchten, und klicken Sie anschließend auf die Schaltfläche **Zugriffsrechte**.

   Sie können nur einzelne Benutzer oder Sicherheitsgruppen auswählen. Wenn Sie mehr als ein Objekt 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 eines anderen Kaspersky-Programms.

   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 **Programmintegration**, um einem Benutzer oder einer Gruppe alle verfügbaren Zugriffsrechte auf die Funktionen der Programmintegration (**Lesen**, **Schreiben** und **Ausführen**) zu gewähren.

      Beispiel 2: Erweitern Sie den Knoten **Verwaltung von Chiffrierschlüsseln** und aktivieren Sie das Kontrollkästchen **Erlauben** neben dem **Schreibzugriff**, um einem Benutzer oder einer Gruppe das Recht **Schreibzugriff** auf die Funktion zur Verwaltung von Chiffrierschlüsseln zu erteilen.

4. Klicken Sie nach der Konfiguration der Zugriffsrechte auf **OK**.

Der Satz der Rechte für den Benutzer oder die Benutzergruppe wird angepasst.

Die Berechtigungen des Administrationsservers (oder der Administrationsgruppe) sind auf die folgenden Bereiche aufgeteilt:

- Allgemeine Funktionen:
  - Verwaltung von Administrationsgruppen
  - Zugriff auf Objekte, unabhängig von deren ACLs
  - Grundlegende Funktionen
  - Gelöschte Objekte
  - Verwaltung der Chiffrierschlüssel
  - Verarbeitung von Ereignissen
  - Vorgänge mit dem Administrationsserver (nur im Eigenschaftenfenster von Administrationsserver)
  - Kaspersky software deployment
  - Verwaltung von Lizenzschlüsseln
  - Programmintegration
  - Erzwungene Berichtsverwaltung
  - Hierarchie des Administrationsservers
  - Benutzerberechtigungen
  - Virtuelle Administrationsserver
- Verwaltung mobiler Geräte:
  - Allgemein

    - Self Service Portal
- Systemverwaltung:
    - Konnektivität
    - Hardware-Inventarisierung
    - Network Access Control
    - Bereitstellung des Betriebssystems
    - Remote-Installation
    - Software-Inventur

Wenn für ein Zugriffsrecht weder **Zulassen** noch **Verbieten** ausgewählt ist, dann gilt das Zugriffsrecht als *Nicht festgelegt*: Es wird verboten bis es für den Benutzer ausdrücklich verboten oder erlaubt wird.

Die Rechte eines Benutzers sind die Summe aus Folgendem:

- Den eigenen Rechten des Benutzers
- Den Rechten aller Rollen, die diesem Benutzer zugewiesen sind
- Den Rechten aller Sicherheitsgruppen, zu denen der Benutzer gehört
- Den Rechten aller Rollen, die den Sicherheitsgruppen zugewiesen sind, zu denen der Benutzer gehört

Wenn zumindest einer dieser Sätze von Rechten für eine Berechtigung **Verbieten** aufweist, erhält der Benutzer diese Berechtigung nicht, selbst wenn sie in anderen Sätze erlaubt oder nicht festgestellt ist.

Benutzerkonto für einen internen Benutzer hinzufügen

Um ein neues internes Benutzerkonto zu Kaspersky Security Center Linux hinzuzufügen:

1. Wechseln Sie im Hauptmenü zu **Benutzer und Rollen** → **Benutzer und Gruppen** und wählen Sie anschließend die Registerkarte **Benutzer** aus.
2. Klicken Sie auf die Schaltfläche **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 Gruppen enthalten:
            - Großbuchstaben (A–Z)

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

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

Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese gedrückt.

Die Anzahl der Eingabeversuche für das Kennwort ist beschränkt. Standardmäßig beträgt die maximale Anzahl der Eingabeversuche für das Kennwort 10. Sie können die zulässige Anzahl der Versuche zur Eingabe eines Kennworts ändern (siehe Beschreibung unter Anzahl der erlaubten Kennworteingabeversuche).

Wenn der Benutzer das Kennwort innerhalb der angegebenen Anzahl von Versuchen nicht korrekt eingegeben hat, wird das Benutzerkonto für eine Stunde gesperrt. Sie können das Benutzerkonto nur durch die Änderung des Kennworts entsperren.

4. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

Ein neues Benutzerkonto wird zur Liste mit Benutzern hinzugefügt.

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 die Schaltfläche **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

Um ein internes Benutzerkonto in Kaspersky Security Center Linux zu bearbeiten:

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, das Sie bearbeiten möchten.

3. Ändern Sie im folgenden Fenster für Benutzereinstellungen auf der Registerkarte **Allgemein** die Einstellungen für das Benutzerkonto:

   - **Beschreibung**
   - **Vollständiger Name**
   - **E-Mail-Adresse**
   - **Hauptrufnummer**
   - **Neues Kennwort festlegen** für die Verbindung des Benutzers mit Kaspersky Security Center Linux an.

     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 Gruppen enthalten:
       - Großbuchstaben (A–Z)
       - Kleinbuchstaben (a–z)
       - Zahlen (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 die Schaltfläche **Anzeigen**.

     Die Anzahl der Eingabeversuche für das Kennwort ist beschränkt. Standardmäßig beträgt die maximale Anzahl der Eingabeversuche für das Kennwort 10. Sie können die zulässige Anzahl an Versuchen ändern, es wird jedoch aus Sicherheitsgründen nicht empfohlen, diese Zahl zu verringern. Wenn der Benutzer das Kennwort innerhalb der angegebenen Anzahl von Versuchen nicht korrekt eingegeben hat, wird das Benutzerkonto für eine Stunde gesperrt. Sie können das Benutzerkonto nur durch die Änderung des Kennworts entsperren.

   - Schalten Sie ggf. die Umschalttaste auf **Deaktiviert**, um zu verhindern, dass der Benutzer eine Verbindung zur Anwendung herstellt. Sie können ein Konto beispielsweise deaktivieren, nachdem ein Mitarbeiter das Unternehmen verlassen hat.

4. Auf der Registerkarte **Sicherheit für die 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. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu speichern.

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. Wechseln 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, wie man einen Benutzer zum Gerätebesitzer macht, entnehmen Sie der Hilfe von Kaspersky Security für mobile Endgeräte.

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 **Assets (Geräte)** → **Verwaltete 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 während der Installation des Administrationsagenten mittels Installationspakets einen Benutzer zum Gerätebesitzer zu ernennen, fügen Sie die in der folgenden Tabelle angegebenen Variablen zu den Einstellungen des Installationspakets des Administrationsagenten hinzu.

Name der Variablen	Notwendig	Beschreibung	Mögl
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 To Registrier Benutzer Geräteb nach der des Administ gestartet Other – D nicht ver
KLNAGENT_DEVICEOWNER_LOGIN	Nein Ja, wenn Sie das Kennwort eingeben	Enthält den Benutzernamen eines Benutzers, der als Gerätebesitzer registriert wird.	Der Benu Benutzer Benutzer Kaspersk Center L angegeb
KLNAGENT_DEVICEOWNER_PASSWORD	Nein Ja, wenn Sie den Benutzernamen eingeben	Enthält das verschlüsselte Kennwort eines Benutzers, der als Gerätebesitzer registriert wird.	Das Kenn Benutzer

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. Weitere Informationen über die Installation im Silent-Modus mit einer Antwortdatei finden Sie in diesem Artikel.

So ernennen während der Installation des Administrationsagent im Silent-Modus mit einer Antwortdatei einen Benutzer zum Gerätebesitzer:

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.

Wenn für den Benutzer die zweistufige Überprüfung aktiviert ist, müssen Sie das zeitbasierte Einmalkennwort (TOTP) aus der App eingeben. Weitere Informationen zur zweistufigen Überprüfung finden Sie in diesem Artikel.

Benutzer nach der Installation des Administrationsagenten zum Gerätebesitzer ernennen

So erlauben Sie dem Benutzer, sich zum Gerätebesitzer zu ernennen:

1. Wechseln Sie in der Kaspersky Security Center Web Console zu **Gerätesuche und Bereitstellung** → **Bereitstellung und Zuweisung** → **Installationspakete**.

   Die Liste mit den Installationspaketen 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 Gerätebesitzer eines 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.

Wenn für den Benutzer die zweistufige Überprüfung aktiviert ist, müssen Sie das zeitbasierte Einmalkennwort (TOTP) aus der App eingeben. Weitere Informationen zur zweistufigen Überprüfung finden Sie in diesem Artikel.

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 des Client-Geräts 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.

Wenn für den Benutzer die zweistufige Überprüfung aktiviert ist, müssen Sie das zeitbasierte Einmalkennwort (TOTP) aus der App eingeben. Weitere Informationen zur zweistufigen Überprüfung finden Sie in diesem Artikel.

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.

Um den Benutzerkonten-Schutz vor unbefugten Änderungen zu aktivieren oder zu deaktivieren:

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 den Benutzerkonten-Schutz vor nicht autorisierten Änderungen anpassen möchten.

3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Sicherheit für die Authentifizierung**.

4. Wählen Sie auf der Registerkarte **Sicherheit für die Authentifizierung** die Option **Authentifizierung anfordern, um zu prüfen, ob Benutzerkonten geändert werden dürfen**, wenn Sie jedes Mal Anmeldedaten anfordern möchten, sobald Benutzerkonto-Einstellungen geändert oder bearbeitet werden. Wählen Sie andernfalls die Option **Benutzern das Ändern des Kontos ohne zusätzliche Authentifizierung erlauben**.

5. Klicken Sie auf **Speichern**.

Zweistufige Überprüfung

In diesem Abschnitt wird beschrieben, wie Sie die zweistufige Überprüfung verwenden können, um das Risiko eines nicht autorisierten Zugriffs auf die Kaspersky Security Center Web Console zu verringern.

Szenario: Konfigurieren der zweistufigen Überprüfung für alle Benutzer

In diesem Szenario wird beschrieben, wie Sie die zweistufige Überprüfung für alle Benutzer aktivieren und wie Benutzerkonten von der zweistufigen Überprüfung ausschließen. Wenn Sie die zweistufige Überprüfung für Ihr Benutzerkonto nicht aktiviert haben, bevor Sie es für andere Benutzer aktivieren, öffnet die Anwendung zunächst das Fenster zur Aktivierung der zweistufigen Überprüfung für Ihr Konto. In diesem Szenario wird außerdem beschrieben, wie Sie die zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktivieren.

Wenn Sie die zweistufige Überprüfung für Ihr Benutzerkonto aktiviert haben, können Sie mit der Aktivierung der zweistufigen Überprüfung für alle Benutzer fortsetzen.

Erforderliche Vorrausetzungen

Vor dem Start:

- Stellen Sie sicher, dass Ihr Benutzerkonto über die Berechtigung "Objekt-ACL ändern" für den Funktionsbereich **Allgemeine Funktionen: Benutzerrechte** verfügt, um die Sicherheitseinstellungen für andere Benutzerkonten zu ändern.
- Stellen Sie sicher, dass die anderen Benutzer des Administrationsservers eine Authenticator-App auf ihren Geräten installieren.

Schritte

Das Aktivieren der zweistufigen Überprüfung für alle Benutzer erfolgt schrittweise:

1. **Installation einer Authenticator-App auf einem Gerät**

   Sie können jedes Programm installieren, das den Algorithmus für zeitbasierte Einmalkennwörter (TOTP) unterstützt, z B:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP

- Yandex Key
- Avanpost Authenticator
- Aladdin 2FA

Um zu überprüfen, ob Kaspersky Security Center Linux die von Ihnen verwendete Authenticator-App unterstützt, aktivieren Sie die zweistufige Überprüfung 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 die Verbindung zum Administrationsserver hergestellt wird.

2. **Synchronisation der Zeit der Authenticator-App mit der Zeit des Gerätes, auf dem der Administrationsserver installiert ist**

   Stellen Sie mithilfe externer Zeitquellen 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. Andernfalls können Fehler bei der Authentifizierung und Aktivierung der zweistufigen Überprüfung auftreten.

3. **Aktivieren der zweistufigen Überprüfung für Ihr Benutzerkonto und Anfordern des geheimen Schlüssels für Ihr Benutzerkonto**

   Nachdem Sie die die zweistufige Überprüfung für Ihr Benutzerkonto aktiviert haben, können Sie die zweistufige Überprüfung für alle Benutzer aktivieren.

4. **Zweistufige Überprüfung für alle Benutzer aktivieren**

   Benutzer, für welche die zweistufige Überprüfung aktiviert ist, müssen diese verwenden, um sich am Administrationsserver anmelden.

5. **Neuen Benutzern die Einrichtung der zweistufigen Überprüfung für sich selbst verbieten**

   Um die Zugriffssicherheit von Kaspersky Security Center Web Console weiter zu verbessern, können Sie verhindern, dass neue Benutzer die zweistufige Überprüfung für sich selbst einrichten.

6. **Den Namen eines Sicherheitscode-Ausstellers bearbeiten**

   Wenn Sie mehrere Administrationsserver mit ähnlichen Namen haben, müssen Sie möglicherweise die Namen der Sicherheitscode-Aussteller ändern, um verschiedene Administrationsserver besser unterscheiden zu können.

7. **Ausschließen der Benutzerkonten, für die Sie die zweistufige Überprüfung nicht aktivieren müssen**

   Bei Bedarf können Sie Benutzerkonten von der zweistufigen Überprüfung ausschließen. Benutzer mit ausgeschlossenen Benutzerkonten müssen sich nicht mittels zweistufiger Überprüfung am Administrationsserver anmelden.

8. **Zweistufige Überprüfung für Ihr eigenes Benutzerkonto konfigurieren**

   Wenn die Benutzer nicht von der zweistufigen Überprüfung ausgeschlossen sind und die zweistufige Überprüfung für deren Benutzerkonten noch nicht konfiguriert ist, müssen sie diese in dem Fenster konfigurieren, das sich bei der Anmeldung an der Kaspersky Security Center Web Console öffnet. Andernfalls können sie nicht entsprechend ihren Rechten auf den Administrationsserver zugreifen.

Ergebnisse

Nach Abschluss dieses Szenarios:

- Die zweistufige Überprüfung ist für Ihr Konto aktiviert.
- Die zweistufige Überprüfung ist für alle Benutzerkonten des Administrationsservers aktiviert, mit Ausnahme der Benutzerkonten, die ausgeschlossenen wurden.

Über die zweistufige Überprüfung für ein Benutzerkonto

Mit Kaspersky Security Center Linux können die Benutzer von Kaspersky Security Center Web Console eine zweistufige Überprüfung verwenden. Wenn die zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktiviert ist, müssen Sie bei jeder Anmeldung an der Kaspersky Security Center Web Console den Benutzernamen, das Kennwort und einen zusätzlichen Einmal-Sicherheitscode eingegeben. Um einen Einmal-Sicherheitscode zu erhalten, benötigen Sie eine Authenticator-App auf einem der Geräte, z. B. auf Ihrem Computer oder mobilen Gerät.

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. Der Aussteller-Name wird als Kennung des Administrationsservers in der Authenticator-App verwendet. Wenn Sie den Namen des Sicherheitscode-Ausstellers ändern, müssen Sie einen neuen geheimen Schlüssel ausstellen und an die Authenticator-App übergeben. Ein Sicherheitscode ist einmalig verwendbar und bis zu 90 Sekunden lang gültig (die genaue Zeit kann variieren).

Jeder Benutzer, für den die zweistufige Überprüfung aktiviert ist, kann den eigenen geheimen Schlüssel erneut ausstellen. Wenn sich ein Benutzer mit dem neu ausgestellten geheimen Schlüssel authentifiziert und diesen zur Anmeldung verwendet, speichert der Administrationsserver den neuen geheimen Schlüssel für das Benutzerkonto. Wenn ein Benutzer einen ungültigen neuen geheimen Schlüssel eingibt, speichert der Administrationsserver diesen neuen geheimen Schlüssel nicht und erachtet den aktuellen geheimen Schlüssel für die Authentifizierung weiterhin als gültig.

> Jede Authentifizierungssoftware, die den Algorithmus für zeitbasierte Einmalkennwörter (Time-based One-time Password – TOTP) unterstützt, ist als Authenticator-App geeignet, z. B. der Google Authenticator. Um den Sicherheitscode zu generieren, müssen Sie die in der Authenticator-App eingestellte Zeit mit der eingestellten Zeit des Administrationsservers synchronisieren.

Um zu überprüfen, ob Kaspersky Security Center Linux die von Ihnen verwendete Authenticator-App unterstützt, aktivieren Sie die Zwei-Faktor-Authentifikation 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.

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.

Es wird dringend empfohlen, dass Sie den geheimen Schlüssel (oder den QR-Code) speichern und an einem sicheren Ort aufbewahren. Auf diese Weise können Sie den Zugriff auf die Kaspersky Security Center Web Console wiederherstellen, falls Sie den Zugriff auf Ihr mobiles Gerät verlieren.

Um die Verwendung von Kaspersky Security Center Linux abzusichern, können Sie die zweistufige Überprüfung für Ihr eigenes Konto und die zweistufige Überprüfung für alle Benutzer aktivieren.

Sie können Benutzerkonten von der zweistufigen Überprüfung ausschließen. Dies kann für Dienstkonten erforderlich sein, die den zur Authentifizierung notwendigen Sicherheitscode nicht empfangen können.

Die zweistufige Überprüfung funktioniert entsprechend den folgenden Regeln:

- Nur ein Benutzerkonto, das die Berechtigung "Objekt-ACL ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** besitzt, kann die zweistufige Überprüfung für alle Benutzer aktivieren.
- Nur ein Benutzer, der die zweistufige Überprüfung für das eigene Konto aktiviert hat, kann die Option zur zweistufigen Überprüfung für alle Benutzer aktivieren.
- Nur ein Benutzer, der die zweistufige Überprüfung für das eigene Konto aktiviert hat, kann andere Benutzerkonten von der Liste mit Benutzern, für welche die zweistufige Überprüfung aktiviert ist, ausschließen.
- Ein Benutzer kann die zweistufige Überprüfung nur für sein eigenes Konto aktivieren.
- Ein Benutzerkonto, das die Berechtigung "Objekt-ACLs ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerrechte** besitzt und das an der Kaspersky Security Center Web Console mittels zweistufiger Überprüfung angemeldet ist, kann die zweistufige Überprüfung in folgenden Fällen für andere Benutzer deaktivieren: 1) Für jeden anderen Benutzer nur dann, wenn die zweistufige Überprüfung für alle Benutzer deaktiviert ist. 2) Für einen Benutzer, der von der Liste der für alle Benutzer aktivierten zweistufigen Überprüfung ausgeschlossen ist.
- Jeder Benutzer, der sich mithilfe der zweistufigen Überprüfung an der Kaspersky Security Center Web Console angemeldet hat, kann den eigenen geheimen Schlüssel erneut ausstellen.
- Sie können die Option zur zweistufigen Überprüfung aller Benutzer für den Administrationsserver aktivieren, mit dem Sie gerade arbeiten. Wenn Sie diese Option auf dem Administrationsserver aktivieren, wird Sie diese Option auch für die Benutzerkonten der virtuellen Administrationsserver aktiviert. Sie aktivieren jedoch nicht die zweistufige Überprüfung für die Benutzerkonten der sekundären Administrationsserver.

Zweistufige Überprüfung für Ihr eigenes Benutzerkonto aktivieren

Sie können die zweistufige Überprüfung nur für Ihr eigenes Konto aktivieren.

Bevor Sie beginnen, die zweistufige Überprüfung für Ihr Konto zu aktivieren, müssen Sie unbedingt sicherstellen, dass auf dem mobilen Gerät eine Authenticator-App installiert ist. Stellen Sie sicher, dass die in der Authenticator-App festgelegte Zeit mit der Zeit auf dem Gerät, auf dem der Administrationsserver installiert ist, synchronisiert wird.

So aktivieren Sie die zweistufige Überprüfung für ein Benutzerkonto:

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 Ihres Benutzerkontos.

3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Sicherheit für die Authentifizierung**:

   a. Wählen Sie die Option **Benutzername, Kennwort und Sicherheitscode abfragen (zweistufige Überprüfung)** aus. Klicken Sie auf **Speichern**.

   b. Klicken Sie im folgenden Fenster der zweistufigen Überprüfung auf **So richten Sie die zweistufige Überprüfung ein**.

      Geben Sie den geheimen Schlüssel in die Authenticator-App ein oder klicken Sie auf **QR-Code anzeigen** und scannen Sie den QR-Code mit der Authenticator-App Ihres des Geräts, um einen einmaligen Sicherheitscode zu erhalten.

   c. Geben Sie im Fenster zur zweistufige Überprüfung den Sicherheitscode an, der von der Authenticator-App generiert wurde, und klicken Sie dann auf **Überprüfen und anwenden**.

4. Klicken Sie auf **Speichern**.

Die zweistufige Überprüfung ist für Ihr Konto aktiviert.

Die erforderliche zweistufige Überprüfung für alle Benutzer aktivieren

Sie können die zweistufige Überprüfung für alle Benutzer des Administrationsservers aktivieren, wenn Ihr Benutzerkonto über die Berechtigung "Objekt-ACL ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** verfügt und wenn Sie sich mittels zweistufiger Überprüfung authentifiziert haben.

So aktivieren Sie die zweistufige Überprüfung für alle Benutzer:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Schalten Sie in der Registerkarte **Sicherheit für die Authentifizierung** des Eigenschaftenfensters den Umschalter für die **zweistufige Überprüfung für alle Benutzer** in die Position "aktiviert".

3. Wenn Sie keine zweistufige Überprüfung für Ihr Benutzerkonto aktiviert haben, öffnet die Anwendung das Fenster zum Aktivieren der zweistufigen Überprüfung für Ihr eigenes Konto.

   a. Klicken Sie im Fenster der zweistufigen Überprüfung auf **So richten Sie die zweistufige Überprüfung ein**.

   b. Geben Sie den geheimen Schlüssel manuell in die Authenticator-App ein oder klicken Sie auf **QR-Code anzeigen** und scannen Sie den QR-Code mit der Authenticator-App Ihres des Geräts, um einen einmaligen Sicherheitscode zu erhalten.

   c. Geben Sie im Fenster zur zweistufige Überprüfung den Sicherheitscode an, der von der Authenticator-App generiert wurde, und klicken Sie dann auf **Überprüfen und anwenden**.

Die zweistufige Überprüfung ist für alle Benutzer aktiviert. Von nun an müssen Benutzer des Administrationsservers, einschließlich der Benutzer, die nach der Aktivierung der zweistufigen Überprüfung hinzugefügt wurden, die zweistufige Überprüfung für ihre Konten konfigurieren. Ausgenommen sind Benutzer, die von der zweistufigen Überprüfung ausgeschlossen sind.

Zweistufige Überprüfung für ein Benutzerkonto deaktivieren

Sie können die zweistufige Überprüfung für Ihr eigenes Benutzerkonto sowie für das Konto eines anderen Benutzers deaktivieren.

Sie können die zweistufige Überprüfung das Konto eines anderen Benutzers deaktivieren, wenn Ihr Benutzerkonto über die Berechtigung Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** verfügt und wenn Sie sich mittels zweistufiger Überprüfung authentifiziert haben.

So deaktivieren Sie die zweistufige Überprüfung für ein Benutzerkonto:

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 die zweistufige Überprüfung deaktivieren möchten. Dies kann Ihr eigenes Benutzerkonto oder das Konto eines anderen Benutzers sein.
3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Sicherheit für die Authentifizierung**.
4. Wählen Sie die Option **Nur Benutzername und Kennwort abfragen**, wenn Sie die zweistufige Überprüfung für ein Benutzerkonto deaktivieren möchten.
5. Klicken Sie auf **Speichern**.

Die zweistufige Überprüfung ist jetzt für das Benutzerkonto deaktiviert.

Wenn sich ein Benutzer nicht mehr mit der zweistufigen Überprüfung an der Kaspersky Security Center Web Console anmelden kann und Sie seinen Zugriff wiederherstellen möchten, deaktivieren Sie die zweistufige Überprüfung für dieses Benutzerkonto und wählen Sie anschließend die Option **Nur Benutzername und Kennwort abfragen** wie oben beschrieben aus. Melden Sie sich anschließend in der Kaspersky Security Center Web Console mit dem Benutzerkonto an, für das Sie die zweistufige Überprüfung deaktiviert haben, und aktivieren Sie die Überprüfung erneut.

Die erforderliche zweistufige Überprüfung für alle Benutzer deaktivieren

Sie können die erforderliche zweistufige Überprüfung für alle Benutzer deaktivieren, wenn die zweistufige Überprüfung für Ihr Benutzerkonto aktiviert ist und Ihr Konto die Berechtigung Objekt-ACL ändern im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** hat. Wenn die zweistufige Überprüfung für Ihr Benutzerkonto nicht aktiviert ist, müssen Sie die zweistufige Überprüfung für Ihr Konto aktivieren, bevor Sie diese für alle Benutzer deaktivieren.

So deaktivieren Sie die zweistufige Überprüfung für alle Benutzer:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Schalten Sie in der Registerkarte **Sicherheit für die Authentifizierung** des Eigenschaftenfensters den Umschalter für die **zweistufige Überprüfung für alle Benutzer** in die Position "deaktiviert".

3. Geben Sie die Anmeldedaten Ihres Benutzerkontos im Authentifizierungsfenster ein.

Die zweistufige Überprüfung ist für alle Benutzer deaktiviert. Die Deaktivierung der zweistufigen Überprüfung für alle Benutzer gilt nicht für bestimmte Konten, für welche die zweistufige Überprüfung zuvor separat aktiviert wurde.

Benutzerkonten von der zweistufigen Überprüfung ausschließen

Sie können Benutzerkonten von der zweistufigen Überprüfung ausschließen, wenn Sie die Berechtigung "Objekt-ACL ändern" im Funktionsbereich **Allgemeine Funktionen: Benutzerberechtigungen** haben.

Wenn ein Benutzerkonto von der Liste der zweistufigen Überprüfung für alle Benutzer ausgeschlossen ist, muss dieser Benutzer die zweistufige Überprüfung nicht verwenden.

Das Ausschließen von Benutzerkonten von der zweistufigen Überprüfung kann für Dienstkonten erforderlich sein, die den Sicherheitscode während der Authentifikation nicht übergeben können.

Wenn Sie bestimmte Benutzerkonten von der zweistufigen Überprüfung ausschließen möchten:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Klicken Sie im Eigenschaftenfenster auf der Registerkarte **Sicherheit für die Authentifizierung** in der Tabelle mit den Ausschlüssen aus der zweistufigen Überprüfung auf die Schaltfläche **Hinzufügen**.

3. Führen Sie in dem neuen Fenster folgende Schritte aus:

   a. Wählen Sie die Benutzerkonten aus, die Sie ausschließen möchten.

   b. Klicken Sie auf die Schaltfläche **OK**.

Die ausgewählten Benutzerkonten werden von der zweistufigen Überprüfung ausgeschlossen.

Zweistufige Überprüfung für Ihr eigenes Benutzerkonto konfigurieren

Wenn Sie sich nach der Aktivierung der zweistufigen Überprüfung zum ersten Mal bei Kaspersky Security Center Linux anmelden, wird das Fenster zur Konfiguration der zweistufigen Überprüfung für Ihr eigenes Benutzerkonto geöffnet.

Stellen Sie sicher, dass auf dem mobilen Gerät eine Authenticator-App installiert ist, bevor Sie die zweistufige Überprüfung für Ihr Konto konfigurieren. Stellen Sie mithilfe externer Zeitquellen 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.

So konfigurieren Sie die zweistufige Überprüfung für Ihr Konto:

1. Generieren Sie mithilfe der Authenticator-App auf dem mobilen Gerät einen einmaligen Sicherheitscode. Führen Sie dazu eine der folgenden Maßnahmen durch:

   - Geben Sie den geheimen Schlüssel manuell in die Authenticator-App ein.
   - Klicken Sie auf **QR-Code anzeigen** und scannen Sie den QR-Code mithilfe der Authenticator-App.

   Auf dem Mobilgerät wird ein Sicherheitscode angezeigt.

2. Geben Sie im Fenster zur Konfiguration der zweistufigen Überprüfung den Sicherheitscode an, der von der Authenticator-App generiert wurde, und klicken Sie anschließend auf **Überprüfen und anwenden**.

Die zweistufige Überprüfung ist für Ihr Konto konfiguriert. Sie können entsprechend Ihren Rechten auf den Administrationsserver zugreifen.

Neuen Benutzern die Einrichtung der zweistufigen Überprüfung für sich selbst verbieten

Um die Zugriffssicherheit von Kaspersky Security Center Web Console weiter zu verbessern, können Sie verhindern, dass neue Benutzer die zweistufige Überprüfung für sich selbst einrichten.

Bei aktivierter Option kann ein Benutzer, für den die zweistufige Überprüfung deaktiviert ist (z B. ein neuer Domänenadministrator) die zweistufige Überprüfung nicht für sich selbst konfigurieren. Auf diese Weise kann ein solcher Benutzer ohne Zustimmung eines weiteren Administrators von Kaspersky Security Center Linux, für den die Zwei-Faktor-Authentifikation bereits aktiviert wurde, nicht am Administrationsserver authentifiziert werden und sich nicht an der Kaspersky Security Center Web Console anmelden.

Diese Option ist verfügbar, wenn die Zweistufige Überprüfung für alle Benutzer aktiviert ist.

So verbieten Sie neuen Benutzern, die zweistufige Überprüfung für sich selbst einzurichten:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Aktivieren Sie im Eigenschaftenfenster auf der Registerkarte **Sicherheit für die Authentifizierung** den Umschalter **Neuen Benutzern die Einrichtung der zweistufigen Überprüfung für sich selbst verbieten**.

Diese Option wirkt sich nicht auf Benutzerkonten aus, die zu den Ausnahmen für die zweistufigen Überprüfung hinzugefügt wurden.

Um einem Benutzer mit deaktivierter zweistufiger Überprüfung den Zugriff auf die Kaspersky Security Center Web Console zu gewähren, deaktivieren Sie vorübergehend die Option **Neuen Benutzern die Einrichtung der zweistufigen Überprüfung für sich selbst verbieten**, fordern Sie den Benutzer auf, die zweistufige Überprüfung zu aktivieren, und aktivieren Sie anschließend die Option wieder.

Neuen geheimen Schlüssel generieren

Sie können nur dann einen neuen geheimen Schlüssel für die zweistufige Überprüfung Ihres Benutzerkontos generieren, wenn Sie sich mithilfe der zweistufigen Überprüfung autorisiert haben.

Um einen neuen geheimen Schlüssel für ein Benutzerkonto zu generieren:

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 neuen geheimen Schlüssel für die zweistufige Überprüfung generieren möchten.
3. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Sicherheit für die Authentifizierung**.
4. Klicken Sie auf der Registerkarte **Sicherheit für die Authentifizierung** auf den Link **Neuen geheimen Schlüssel generieren**.
5. Geben Sie im angezeigten Fenster zur zweistufigen Überprüfung einen neuen Sicherheitsschlüssel an, der von der Authenticator-App generiert wird.
6. Klicken Sie auf die Schaltfläche **Überprüfen und anwenden**.

Für den Benutzer wird ein neuer geheimer Schlüssel generiert.

Wenn Sie das Mobilgerät verlieren, können Sie auf einem anderen Mobilgerät eine Authenticator-App installieren und einen neuen geheimen Schlüssel generieren, um den Zugriff auf die Kaspersky Security Center Web Console wiederherzustellen.

Name eines Sicherheitscode-Ausstellers bearbeiten

Möglicherweise haben Sie mehrere Identifikatoren (auch "Aussteller" genannt) für verschiedene Administrationsserver. 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.

Nachdem Sie den Namen des Sicherheitscode-Ausstellers geändert haben, müssen Sie einen neuen geheimen Schlüssel ausstellen und an die Authenticator-App übergeben.

So geben Sie einen neuen Namen des Sicherheitscode-Ausstellers an:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.
2. Öffnen Sie im folgenden Fenster mit den Benutzereinstellungen die Registerkarte **Sicherheit für die Authentifizierung**.
3. Klicken Sie auf der Registerkarte **Sicherheit für die Authentifizierung** auf den Link **Bearbeiten**.

Der Abschnitt **Aussteller des Sicherheitscodes ändern** wird geöffnet.

4. Geben Sie einen neuen Namen für den Sicherheitscode-Aussteller an.
5. Klicken Sie auf die Schaltfläche **OK**.

Für den Administrationsserver wird jetzt ein neuer Name des Sicherheitscode-Ausstellers angezeigt.

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.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Klicken Sie im folgenden Fenster auf **OK**.

Der Benutzer oder die Sicherheitsgruppe ist gelöscht.

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 Programme von Kaspersky.
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 Programme von Kaspersky.
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. Wechseln 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.

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. Wechseln 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 und Profile**.
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 den Richtungspfeil (›) 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.

Kennwort des Benutzerkontos ändern

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.

Die Kennwortänderung ist auch dann wirksam, wenn sich der Benutzer nicht im Konto angemeldet hat. 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 Geräten:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **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 Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen festlegen oder eine neue erstellen.

     Sie können diese Option beispielsweise zum Starten einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die in einer bestimmten Administrationsgruppe enthalten sind.

   - 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.

Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Vielleicht wollen 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 Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen festlegen.

  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 das 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.

     Um die von Ihnen eingegebenen Zeichen anzuzeigen, klicken Sie die Schaltfläche **Anzeigen** und halten Sie diese 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 nicht aktiviert.

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 Aufgaben-Parameter überprüfen, ändern oder bei Bedarf einen Zeitplan für den Start der 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 in den Aufgabeneinstellungen festgelegten Zeitplan gestartet wird.

Nach Abschluss der Aufgabe zum Ändern des Kennworts des Benutzerkontos wird das Kennwort für das angegebene lokale Konto auf den angegebenen Geräten geändert.

Um sicherzustellen, dass die Aufgaben zum Ändern des Kennwort des Benutzerkontos korrekt ausgeführt werden, muss SELinux auf dem Benutzergerät deaktiviert sein.

Lokale Administratorrechte entziehen

Sie können den Benutzerkonten lokale Administratorrechte entziehen. Dadurch erhalten Sie weitere 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 auf ausgewählten Geräten die lokalen Administratorrechte:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **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 Geräten zugewiesen, die in einer Administrationsgruppe enthalten sind. Sie können eine der vorhandenen Gruppen festlegen oder eine neue erstellen.

     Sie können diese Option beispielsweise zum Starten einer Aufgabe zum Senden einer Meldung an Benutzer verwenden, wenn die Meldung spezifisch für Geräte ist, die in einer bestimmten Administrationsgruppe enthalten sind.

   - **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.

Sie können diese Option beispielsweise zur Ausführung einer Aufgabe für ein bestimmtes Subnetz verwenden. Vielleicht wollen 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 Geräten zugewiesen, die in einer Geräteauswahl enthalten sind. Sie können eine der vorhandenen Auswahlen festlegen.

  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 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 Variante ist standardmäßig ausgewählt.

     - **Aufgelistete Benutzerkonten vom Widerruf der lokalen Administratorrechte ausschließen**

       Wenn diese Option ausgewählt ist, die lokalen Administratorrechte von allen lokalen Benutzerkonten außer den angegeben entzogen.

       Diese Variante ist standardmäßig nicht ausgewählt.

   - Geben Sie die lokalen Benutzerkonten an:

     - Klicken Sie auf die Schaltfläche **Hinzufügen**.

     - Führen Sie neuen 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) die Aktion aus.

       - **Benutzerkonto beibehalten**

Wenn diese Option ausgewählt ist, wird das lokale Benutzerkonto nicht gelöscht, nachdem die lokalen Administratorrechte entzogen wurden.

Diese Variante 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 Aufgaben-Parameter überprüfen, ändern oder bei Bedarf einen Zeitplan für den Start der 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 in den Aufgabeneinstellungen festgelegten Zeitplan gestartet wird.

Wenn die Aufgabe zum Entziehen lokaler Administratorrechte abgeschlossen ist, wurden den angegebenen lokalen Benutzerkonten auf den angegebenen Geräten die lokalen Administratorrechte entzogen.

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 Programme von Kaspersky, einschließlich der Komponenten von Kaspersky Security Center Linux und der Sicherheitsanwendungen

Szenario: Datenbanken und Programme von Kaspersky regelmäßig aktualisieren

Dieser Abschnitt enthält ein Szenario zum regelmäßigen Update der Kaspersky-Datenbanken, Softwaremodule und Programme. 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 Programme von Kaspersky, 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 Programme von Kaspersky, 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-Programmen 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 Programme 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 **Updates verteilen** 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 Programme, um zeitnahe Updates für die Programm-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 Ihr Netzwerk ausschließlich IPv6-Geräte enthält und Sie die auf den Geräten installierten Sicherheitsanwendungen regelmäßig aktualisieren möchten, stellen Sie sicher, das auf den verwalteten Geräten der Administrationsserver Version 13.2 oder höher und der Administrationsagent Version 13.2 oder höher installiert sind.

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 Software-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-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 Software-Updates

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 Programme von Kaspersky, einschließlich der Komponenten von Kaspersky Security Center Linux und der Sicherheitsanwendungen

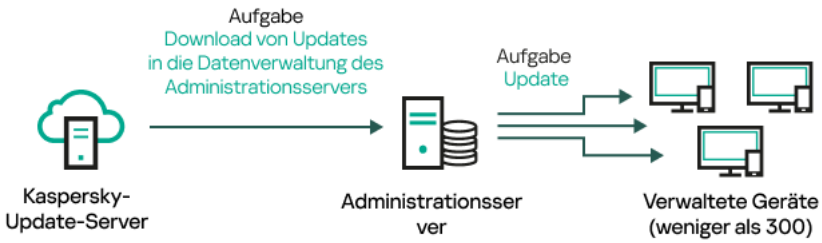
Kaspersky Security Center Linux ermöglicht Ihnen die automatische Aktualisierung des Administrationsagenten und der Kaspersky-Anwendungen auf Windows-Geräten. Eine nahtlose Aktualisierung wird von den folgenden Komponenten nicht unterstützt: Administrationsserver, Kaspersky Security Center Web Console 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).



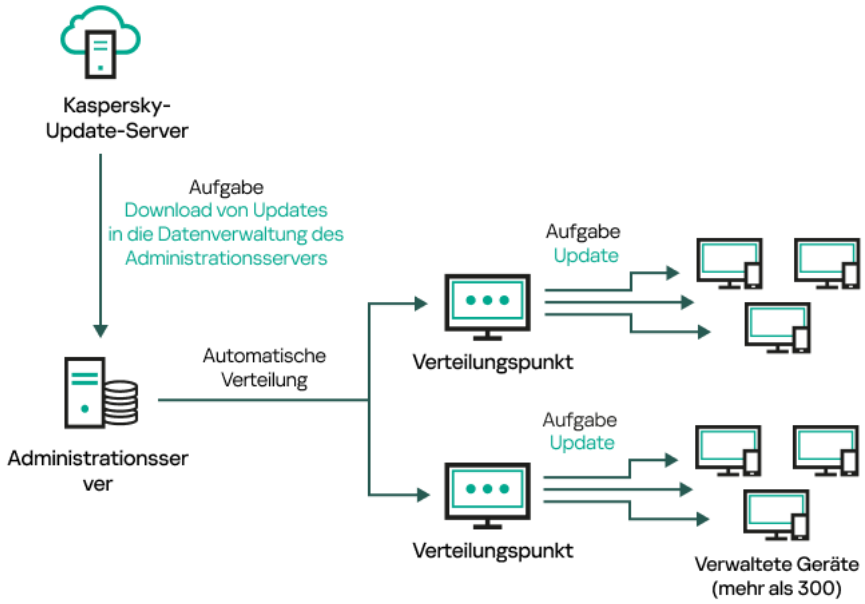
Update mithilfe der Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* ohne Verteilungspunkte

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.

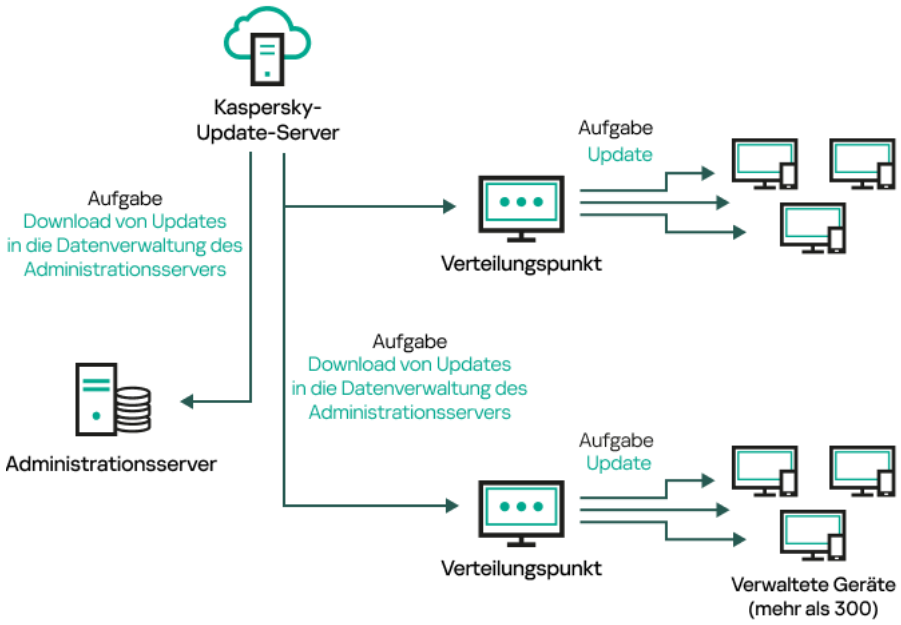
Jede Anwendung von Kaspersky fordert die erforderlichen Updates vom Administrationsserver an. Der Administrationsserver aggregiert diese Anforderungen und lädt nur die Aktualisierungen herunter, die von einer Anwendung angefordert werden. Dadurch wird sichergestellt, dass die gleichen Updates nicht mehrmals 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 des Programms
- Programm-Setup-ID
- 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*

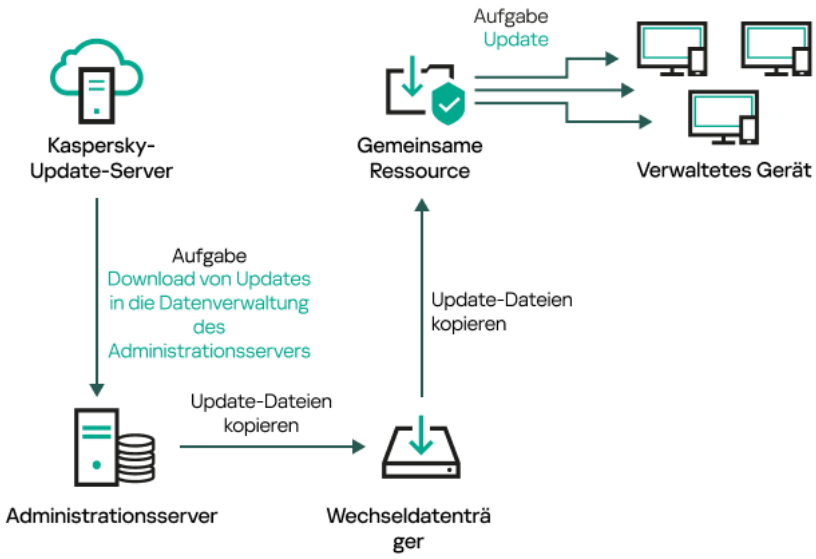
Standardmäßig verwenden der Administrationsserver und die Verteilungspunkte zur Kommunikation mit den Kaspersky-Update-Servern und zum Download von Updates das HTTPS-Protokoll. Sie können den Administrationsserver und/oder die Verteilungspunkte so konfigurieren, dass das HTTP-Protokoll anstelle des HTTPS-Protokolls 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).



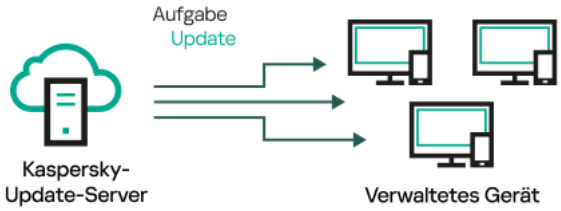
Manuelles Upgrade über einen lokalen Ordner, einen freigegebenen Ordner oder einen FTP-Server

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 Sicherheits-App 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

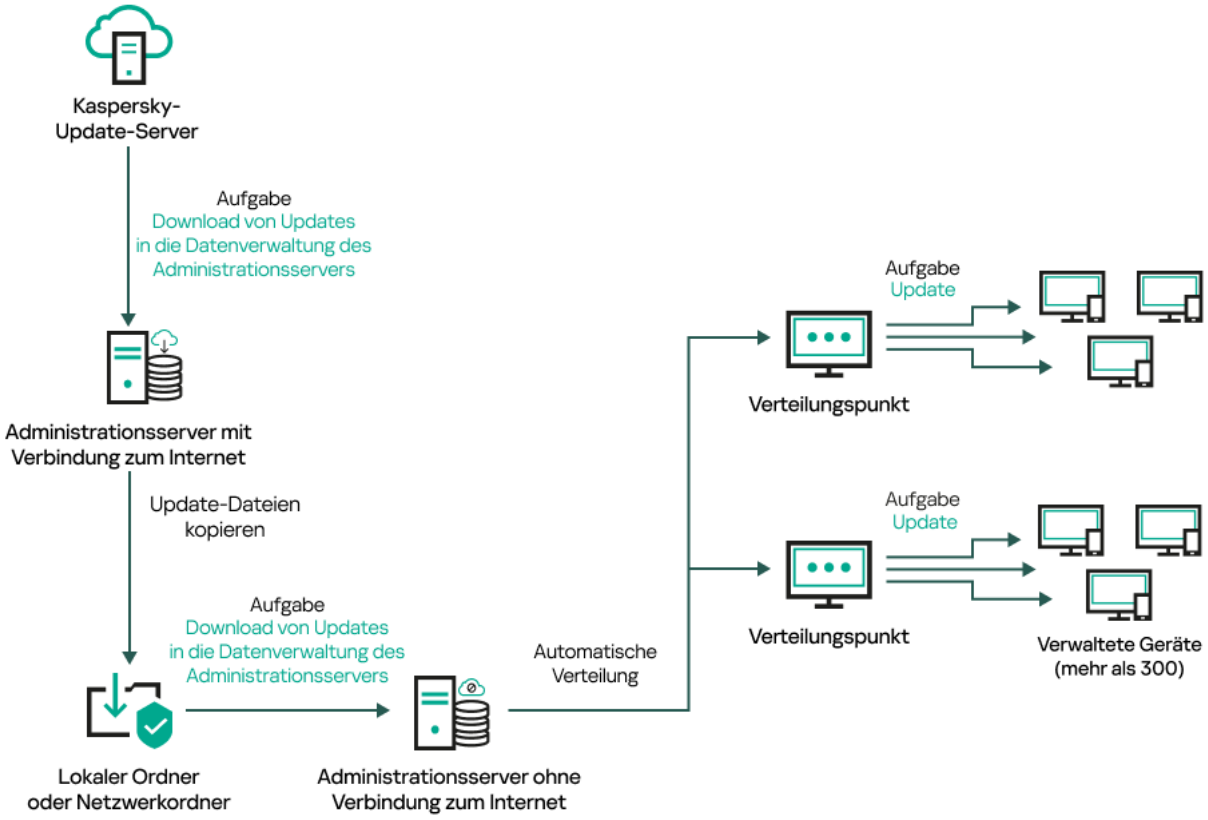
Über einen lokalen Ordner oder Netzwerkordner, wenn der Administrationsserver keine Internetverbindung hat

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*.

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 Programm-Module 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 **Assets (Geräte)** → **Aufgaben**.
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 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.
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.
6. Klicken Sie auf die Schaltfläche **Fertigstellen**.

   Die Aufgabe wird erstellt und in der Aufgabenliste 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 **Programmeinstellungen** die folgenden Einstellungen an:

   - Update-Quellen

Sie können als Update-Quelle die Kaspersky-Update-Server, einen lokalen oder Netzwerkordner oder einen primären Administrationsserver verwenden.

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. Andernfalls 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.

  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 das Programm 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 einem der folgenden Programme 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.

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.

- **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.

- **Täglich (Sommerzeit wird nicht unterstützt)**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

  Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Abwärtskompatibilität von Kaspersky Security Center Linux benötigt.

  Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Wöchentlich**

  Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit 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, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig sind keine Tage des Monats ausgewählt. Die Standardstartzeit beträgt 18:00 Uhr.

- **Nach Beenden 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**.

- 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 des Programms von Kaspersky 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 anhalten, 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.

10. Klicken Sie auf die Schaltfläche **Speichern**.

    Die Aufgabe wird erstellt und konfiguriert.

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 von 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 im Kaspersky-Programm 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 Programmkonfiguration 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 ein von Kaspersky Security Center Linux unterstütztes Programm, 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 **Assets (Geräte)** → **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 **Programmeinstellungen** und aktivieren Sie anschließend die Option **Update-Prüfung ausführen**.

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 zum Hinzufügen von Aufgaben einen Aufgabennamen an, wenn Sie den voreingestellten Namen ändern möchten.

   c. Wählen Sie die zuvor erstellte Administrationsgruppe mit den Testgeräten aus.

   d. Wählen Sie für ein erforderliches Programms, das von Kaspersky Security Center Linux unterstützt wird, zunächst die Update-Aufgabe und anschließend die Aufgabe zur Schadsoftware-Untersuchung aus.

   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.

   e. 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 **Assets (Geräte)** → **Aufgaben**.
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 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.
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 die Schaltfläche **Erstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.
8. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.
9. Geben Sie auf der Registerkarte **Programmeinstellungen** 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 Programme von Kaspersky Updates für Datenbanken und Programm-Module herunterladen.

  Diese Variante ist standardmäßig festgelegt.

- Primärer Administrationsserver

  Diese Ressource gilt für Aufgaben, die für einen sekundären oder virtuellen Administrationsserver erstellt wurden.

- 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 das Programm 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 einem der folgenden Programme 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.

- **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.

- **Täglich (Sommerzeit wird nicht unterstützt)**

  Die Aufgabe wird regelmäßig im festgelegten Intervall in Tagen ausgeführt. In diesem Zeitplan wird die Einhaltung der Sommerzeit nicht unterstützt. Das bedeutet, wenn die Uhren zu Beginn oder am Ende der Sommerzeit eine Stunde vor- oder zurückgestellt werden, ändert sich die tatsächliche Startzeit der Aufgabe nicht.

  Es wird nicht empfohlen, diesen Zeitplan zu verwenden. Er wird für die Abwärtskompatibilität von Kaspersky Security Center Linux benötigt.

  Standardmäßig wird die Aufgabe jeden Tag zur aktuellen Systemzeit gestartet.

- **Wöchentlich**

  Die Aufgabe wird jede Woche am festgelegten Tag und zur festgelegten Uhrzeit 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, an angegebenen Tagen der gewählten Wochen**

  Die Aufgabe wird regelmäßig an den festgelegten Tagen des Monats zur festgelegten Uhrzeit ausgeführt.

  Standardmäßig sind keine Tage des Monats ausgewählt. Die Standardstartzeit beträgt 18:00 Uhr.

- **Beim Erkennen eines Virenangriffs**

Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Programmtypen aus, die Virenangriffe überwachen. Es sind folgende Programmtypen verfügbar:

- Antiviren-Programme für Workstations und Dateiserver
- Anti-Virus für Perimeterschutz
- Anti-Virus für E-Mailsysteme

Standardmäßig sind alle Programmtypen ausgewählt.

Sie können abhängig vom Anti-Virus-Programmtyp, der einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Programmtypen, die Sie nicht benötigen.

- **Nach Beenden 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 des Programms von Kaspersky 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 Angabe eines lokalen Ordners müssen Sie einen Ordner angeben, der sich auf dem Gerät mit dem installierten Administrationsserver befindet. Bei Angabe eines Netzwerkordners können Sie einen FTP- oder HTTP-Server oder eine SMB-Freigabe angeben. Wenn für eine SMB-Freigabe eine Authentifizierung erforderlich ist, muss diese zuvor mit den erforderlichen Anmeldeinformationen im System eingehängt (mount) werden. Es wird davon abgeraten, das SMB1-Protokoll zu verwenden, da es unsicher ist.

Falls ein freigegebener Ordner mit Updates passwortgeschützt ist, aktivieren Sie die Option **Benutzerkonto für den Zugriff auf den freigegebenen Ordner der Update-Quelle angeben (falls vorhanden)** und geben Sie die für den Zugriff erforderlichen Anmeldeinformationen ein.

Um die Update-Quellen hinzuzufügen:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Download von Updates in die Datenverwaltung des Administrationsservers**.
3. Gehen Sie zur Registerkarte **Programmeinstellungen**.
4. Klicken Sie in der Tabelle Update-**Update-Quellen** die Schaltfläche **Hinzufügen**.
5. Fügen Sie im angezeigten Fenster die erforderlichen 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 den lokalen Ordner oder den Netzwerkordner hinzufügen, können Sie Prioritäten für die Updates festlegen. Aktivieren Sie dazu in der Tabelle Update-**Update-Quellen** das Kontrollkästchen neben dem Update, dessen Priorität Sie ändern möchten, und klicken Sie dann auf die Schaltfläche Nach **Nach oben** oder **Nach unten**.

Genehmigen und Ablehnen von Software-Updates

Die Einstellungen einer Aufgabe zur Installation von Updates 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 zuerst die Installation von Updates in einer Testumgebung überprüfen und sich vergewissern, dass sie den Betrieb von Geräten nicht stören, und erst dann die Installation dieser Updates auf Client-Geräten erlauben.

Das Genehmigen und Ablehnen von Updates ist nur für Administrationsagenten und verwaltete Anwendungen verfügbar, die auf Windows-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. Um diese Komponenten zu aktualisieren, müssen Sie die jeweils aktuellste Version von der Kaspersky-Website herunterladen und anschließend manuell installieren.

Um ein oder mehrere Updates zu genehmigen oder abzulehnen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge → Programme von Kaspersky → Nahtlose Updates**.

   Eine Liste verfügbarer Updates wird geöffnet.

   Für Updates verwalteter Anwendungen muss möglicherweise eine bestimmte Mindestversion von Kaspersky Security Center installiert werden. 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, bis Sie Kaspersky Security Center aktualisiert haben. Sie werden aufgefordert, Ihre Kaspersky Security Center-Instanz auf die erforderliche Mindestversion zu aktualisieren.

2. Akzeptieren Sie gegebenenfalls die EULA, indem Sie auf die Schaltfläche **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.

   Als Standard gilt der Wert *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, (falls möglich) deinstalliert. Ferner werden sie in Zukunft nicht auf anderen Geräten installiert.

Einige Updates für die Programme von Kaspersky können nicht deinstalliert werden. Wenn Sie für diese den Status *Abgelehnt* für festlegen, wird Kaspersky Security Center Linux diese Updates nicht von den Geräten deinstallieren, auf denen sie zuvor installiert waren. Diese Updates werden jedoch in Zukunft niemals auf anderen Geräten installiert.

Wenn Sie den Status *Deaktiviert* für Software-Updates von Drittanbietern angeben, werden die Updates nicht auf den Geräten installiert, auf denen sie vorgesehen waren, aber auf denen sie noch nicht installiert wurden. Auf den Geräten, auf denen die Updates bereits installiert wurden, bleiben diese auch weiterhin. Wenn Sie diese Updates löschen müssen, können Sie diese lokal manuell löschen.

Automatische Installation von Updates für Kaspersky Endpoint Security für Windows

Sie können das automatische Datenbanken-Update und das Update der Programm-Module von Kaspersky Endpoint Security für Windows auf den Client-Geräten konfigurieren.

Um den Download und die automatische Installation von Updates für Kaspersky Endpoint Security für Windows auf den Geräten zu konfigurieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Aufgaben**.
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 für die Anwendung Kaspersky Endpoint Security für Windows als Aufgabenuntertyp **Update**.
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 den Aufgabenbereich aus.
6. Legen Sie die Administrationsgruppe, die Geräteauswahl oder die Geräte, für die Aufgabe gilt, fest.
7. 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.
8. Klicken Sie auf die Schaltfläche **Erstellen**.

   Daraufhin wird die importierte Aufgabe in der Aufgabenliste erstellt und angezeigt.
9. Klicken Sie auf den Namen der erstellten Aufgabe, um das Fenster mit den Aufgabeneigenschaften zu öffnen.
10. Definieren Sie auf der Registerkarte **Programmeinstellungen** im Aufgabeneigenschaftenfenster die Einstellungen der Update-Aufgabe im lokalen oder mobilen Modus:

    - **Lokaler Modus**: zwischen dem Gerät und Administrationsserver ist eine Verbindung hergestellt.
    - **Mobiler Modus**: zwischen Kaspersky Security Center Linux und dem Gerät besteht keine Verbindung (wenn beispielsweise das Gerät nicht mit dem Internet verbunden ist).
11. Aktivieren Sie die Update-Quellen, die Sie verwenden möchten, um Datenbanken und Programm-Module für Kaspersky Endpoint Security für Windows zu aktualisieren. Ändern Sie bei Bedarf die Positionen der Quellen in der Liste mit den Tasten **Nach oben** und **Nach unten**. Wenn mehrere Update-Quellen aktiviert sind, versucht Kaspersky Endpoint Security für Windows, sich nacheinander mit ihnen zu verbinden, beginnend am Anfang der Liste, und führt die Update-Aufgabe aus, indem es das Update-Paket von der ersten verfügbaren Quelle abruft.
12. Aktivieren Sie die Option **Genehmigte Updates für Programm-Module installieren**, um die Updates für die Programm-Module einmalig von 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 aktiviert während der Ausführung der Update-Aufgabe das Update der Programm-Module im Update-Paket. 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 Programm-Module automatisch installieren** aktivieren. Wenn Updates für die Programm-Module verfügbar sind, installiert Kaspersky Endpoint Security für Windows alle Updates mit dem Status *Kritisch* automatisch; die restlichen Updates werden installiert, nachdem Sie diese genehmigt haben.

Wenn für es für das Update von Programm-Modulen erforderlich ist, dass sich der Benutzer mit den Bedingungen des Lizenzvertrags und Datenschutzrichtlinie vertraut macht und diese akzeptiert, werden die Updates installiert, nachdem der Benutzer die Bedingungen des Lizenzvertrags und der Datenschutzrichtlinie akzeptiert hat.

13. Aktivieren Sie das Kontrollkästchen **Updates in Ordner kopieren**, damit das Programm die heruntergeladenen Updates in einen Ordner kopiert, und geben Sie den Pfad an.

14. Planen Sie die Aufgabe. Um zeitnahe Updates sicher zu stellen, wird empfohlen, die Option **Nach dem Download von Updates in die Datenverwaltung** auszuwählen.

15. Klicken Sie auf die Schaltfläche **Speichern**.

Beim Ausführen der Aufgabe **Update** sendet das Programm Anfragen an die Kaspersky-Update-Server.

Einige Updates erfordern die Installation aktueller 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 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 überbrücken 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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 **Aufgaben 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. Dieses Programm 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: \\<Servername>\KLSHARE\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.

Web-Plugins sichern und wiederherstellen

Mit Kaspersky Security Center Web Console können Sie den aktuellen Zustand eines Web-Plug-ins sichern, um den gespeicherten Zustand später wiederherstellen zu können. Beispielsweise können Sie ein Web-Plug-in sichern, bevor Sie es auf eine neuere Version aktualisieren. Wenn die neuere Version nach dem Update nicht Ihren Anforderungen oder Erwartungen entspricht, können Sie die vorherige Version des Web-Plug-ins aus dem Backup wiederherstellen.

So sichern Sie Web-Plug-Ins:

1. Wechseln Sie im Hauptmenü zu **Einstellungen** → **Web-Plug-ins**.
2. Wählen Sie im Abschnitt **Web-Plug-ins** die Web-Plug-ins aus, die Sie sichern möchten, und klicken Sie anschließend auf die Schaltfläche **Backup-Kopie erstellen**.

Die ausgewählten Web-Plug-ins werden gesichert. Sie können die erstellten Backups im Abschnitt **Backups** anzeigen.

So stellen Sie ein Web-Plug-in aus einem Backup wieder her:

1. Wechseln Sie im Hauptmenü zu **Einstellungen** → **Backups**.

2. Wählen Sie im Abschnitt **Backups** das Backup von dem Web-Plug-in aus, welches Sie wiederherstellen möchten, und klicken Sie anschließend auf die Schaltfläche **Aus Backup wiederherstellen**.

Das Web Plug-in wird aus dem ausgewählten Backup wiederhergestellt.

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 Programme werden vom Client-Gerät übertragen und in der Datenbank des Administrationsservers 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 Adaptive Kontrolle von Anomalien und Funden, die von Regeln für die Adaptive Kontrolle von Anomalien in Kaspersky Endpoint Security für Windows auf Client-Geräten durchgeführt wird.

Die Regeln finden abnormales Verhalten auf Client-Geräten und können dieses blockieren. Wenn die Regeln im Smart Training-Modus ausgeführt werden, erkennen sie abnormales Verhalten und senden Berichte über jeden Fund an den Administrationsserver. Diese Informationen werden als Liste im Unterordner **Auslösen von Regeln im Smart-Training-Status** des Ordners **Datenverwaltung** gespeichert. Sie können Funde als korrekt bestätigen oder sie als Ausschlüsse hinzufügen, damit solches Verhalten in der Zukunft nicht als anomal registriert wird.

Informationen über Funde werden im Ereignisprotokolle 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 der Liste der Funde mithilfe der Regeln für die Adaptive Kontrolle von Anomalien

So zeigen Sie die Liste der Funde mithilfe der Regeln für die Adaptive Kontrolle von Anomalien an:

1. Wählen Sie in der Konsolenstruktur den Knoten des erforderlichen Administrationsservers aus.
2. Wählen Sie den Unterordner **Auslösen von Regeln im Smart-Training-Status** aus (standardmäßig ist dies ein Unterordner von **Erweitert** → **Datenverwaltung**).

   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.

   - **Gerätename**

     Name des Client-Geräts, auf dem die Regel übernommen wurde.

   - **Name**

     Name der Regel, die übernommen wurde.

   - **Status**

     Ausschluss wird erstellt – Wenn der Administrator dieses Element verarbeitet und als Ausschluss aus den 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.

     Bestätigung – 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 Regelauslösungen**

     Anzahl der Funde innerhalb einer heuristischen Regel, eines Prozesses und eines Client-Geräts. 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. zum Prozess, der diese 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.

Um Eigenschaften der einzelnen Informationselemente anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten des erforderlichen Administrationsservers aus.
2. Wählen Sie den Unterordner **Auslösen von Regeln im Smart-Training-Status** aus (standardmäßig ist dies ein Unterordner von **Erweitert** → **Datenverwaltung**).
3. Wählen Sie im Arbeitsbereich **Auslösen von Regeln im Smart-Training-Status** das gewünschte Objekt aus.
4. Führen Sie eine der folgenden Aktionen aus:

   - Klicken Sie im Informationsfeld auf der rechten Bildschirmseite auf den Link **Eigenschaften**.

- Drücken Sie die rechte Maustaste und wählen Sie im Kontextmenü **Eigenschaften** aus.

Daraufhin wird das Eigenschaftenfenster des Objekts geöffnet und zeigt Informationen über das ausgewählte Element an.

Sie können jedes Element in der Liste mit Funden der Regeln zur Adaptiven Kontrolle von Anomalien bestätigen oder zu den Ausschlüssen hinzufügen.

Um ein Element zu bestätigen, gehen Sie wie folgt vor:

Klicken Sie auf ein Element (oder mehrere Elemente) in der Liste der Funde und anschließend auf die Schaltfläche **Bestätigen**.

Der Status der Elemente wird in **Bestätigung** geändert.

Ihre Bestätigung trägt zu den Statistiken bei, die von den Regeln verwendet werden (weitere Informationen finden Sie in der Hilfe zu Kaspersky Endpoint Security 11 für Windows).

Um ein Element als Ausschluss hinzuzufügen, gehen Sie wie folgt vor:

klicken Sie mit der rechten Maustaste auf ein Element (oder mehrere Elemente) in der Liste der Funde und wählen Sie im Kontextmenü **Zu Ausschlüssen hinzufügen** aus.

Daraufhin wird der Assistent für das Hinzufügen eines Ausschlusses gestartet. Folgen Sie den Anweisungen des Assistenten.

Wenn Sie ein Element ablehnen oder bestätigen, wird es nach der nächsten Synchronisierung des Client-Geräts mit dem Administrationsserver von der Liste der Funde von adaptiven Anomalien ausgeschlossen und nicht länger in der Liste angezeigt.

Ausschlüsse aus den Regeln zur Adaptiven Kontrolle von Anomalien hinzufügen

Der Assistent für das Hinzufügen eines Ausschlusses erlaubt das Hinzufügen von Ausnahmen aus den Regeln zur Adaptiven Kontrolle von Anomalien für Kaspersky Endpoint Security.

Sie können den Assistenten durch eine der folgenden drei Prozeduren starten.

Um den Assistent für das Hinzufügen eines Ausschlusses über den Knoten "Adaptive Kontrolle von Anomalien" zu starten, gehen Sie wie folgt vor:

1. Wählen Sie in der Konsolenstruktur den Knoten des gewünschten Administrationsservers aus.
2. Wählen Sie **Auslösen von Regeln im Smart-Training-Status** (standardmäßig ist dies ein Unterordner von **Erweitert** → **Datenverwaltung**).
3. Klicken Sie im Arbeitsbereich mit der rechten Maustaste auf ein Element (oder mehrere Elemente) in der Liste der Funde und wählen Sie **Zu Ausschlüssen hinzufügen**.

   Sie können bis zu 1000 Ausschlüsse auf einmal hinzufügen. Wenn Sie mehr Elemente auswählen und versuchen, sie zu den Ausschlüssen hinzuzufügen, wird eine Fehlermeldung angezeigt.

Daraufhin wird der Assistent für das Hinzufügen eines Ausschlusses gestartet. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

Der Assistent für das Hinzufügen eines Ausschlusses kann aus anderen Knoten der Konsolenstruktur gestartet werden:

- Registerkarte **Ereignisse** des Hauptfensters des Administrationsservers (Option **Benutzeranfragen** oder **Letzte Ereignisse**).
- Spalte **Bericht zum Regelstatus der Adaptiven Kontrolle von Anomalien**, **Anzahl der Funde**.

So fügen Sie Ausnahmen mithilfe des Assistent für das Hinzufügen eines Ausschlusses zu den Regeln der Adaptiven Kontrolle von Anomalien hinzu:

1. Wählen Sie im ersten Schritt des Assistenten eine Anwendung aus der Liste der Kaspersky-Anwendungen aus, deren Verwaltungs-Plug-ins es Ihnen ermöglichen, Ausnahmen zu den Richtlinien für dieser Anwendungen hinzuzufügen.

   Dieser Schritt kann übersprungen werden, wenn Sie nur über ein Kaspersky Endpoint Security für Windows verfügen und keine anderen Anwendungen haben, welche die Regeln für die Adaptive Kontrolle von Anomalien verwenden.

2. Wählen Sie alle Richtlinien und Profile aus, denen Sie Ausschlüsse hinzufügen möchten.

   Im nächsten Schritt wird während der Verarbeitung der Richtlinien ein Fortschrittsbalken angezeigt. Sie können die Verarbeitung von Richtlinien unterbrechen, indem Sie auf **Abbrechen** klicken.

   Geerbte Richtlinien können nicht aktualisiert werden. Wenn Sie keine Berechtigungen zum Ändern einer Richtlinie verfügen, wird diese Richtlinie ebenfalls nicht aktualisiert.

   Wenn alle Richtlinien verarbeitet wurden (oder wenn Sie die Verarbeitung unterbrechen), wird ein Bericht angezeigt. Dieser zeigt, welche Richtlinien erfolgreich aktualisiert wurden (grünes Symbol) und welche Richtlinien nicht aktualisiert wurden (rotes Symbol).

3. Klicken Sie auf **Fertigstellen**, um den Assistenten zu schließen.

   Der Ausschluss von den Regeln der Adaptiven Kontrolle von Anomalien ist 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 und Berichterstattung** 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 und Berichterstattung** → **Dashboard**.
2. Klicken Sie auf die Schaltfläche **Web-Widget hinzufügen oder wiederherstellen**.
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 den Richtungspfeil (>) neben dem Kategorienamen.
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. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.

2. Klicken Sie auf das Einstellungen-Symbol (⚙) neben dem Widget, das Sie ausblenden möchten.
3. Wählen Sie **Web-Widget verbergen** 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. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **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 und Berichterstattung** → **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 und Berichterstattung** → **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:

- **Gültigkeitsbereich des Web-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.
- **Werte mit Status "Kritisch"** und **Werte mit Status "Warnung"** (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 und Berichterstattung** → **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 und Berichterstattung → 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-Programmen spezielle Zugriffsrechte benötigt, konfigurieren Sie diese Rechte für den Benutzer. Anschließend werden für den Benutzer die Daten der Kaspersky-Programme in ihren entsprechenden Programm-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.

Berichte

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 und Berichterstattung** 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. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → 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.
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.
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.
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.

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 und Berichterstattung** → **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.
4. Bearbeiten Sie die Berichtsvorlageneigenschaften:

   - 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 aufnehmen**

  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.

Exportieren eines Berichts in eine Datei

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 und Berichterstattung → Berichte**.
2. Wählen Sie die Berichte aus, die Sie exportieren möchten.

   Wenn Sie mehr als 10 Berichte auswählen, wird die Schaltfläche **Bericht exportieren** deaktiviert.
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 das Programm, dass dieses Tool auf dem Administrationsserver-Gerät installiert werden muss. Installieren Sie das Tool manuell und gehen Sie dann zum nächsten Schritt.
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 und Berichterstattung → 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 und Berichterstattung → 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. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
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 das Programm, 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 in einem Ordner gespeichert werden sollen; ob zuvor gespeicherte Berichte in diesem Ordner überschrieben werden sollen; ob ein bestimmtes Benutzerkonto für den Zugriff auf den Ordner verwendet werden soll (bei freigegebenen Ordnern).

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 sind keine Tage des Monats ausgewählt. Die Standardstartzeit beträgt 18:00 Uhr.

- **Beim Erkennen eines Virenangriffs**

  Die Aufgabe wird ausgeführt, nachdem das Ereignis *Virenangriff* auftritt. Wählen Sie Programmtypen aus, die Virenangriffe überwachen. Es sind folgende Programmtypen verfügbar:

  - Antiviren-Programme für Workstations und Dateiserver
  - Anti-Virus für Perimeterschutz
  - Anti-Virus für E-Mailsysteme

  Standardmäßig sind alle Programmtypen ausgewählt.

  Sie können abhängig vom Anti-Virus-Programmtyp, der einen Virenangriff meldet, unterschiedliche Aufgaben ausführen. Entfernen Sie in diesem Fall die Auswahl der Programmtypen, die Sie nicht benötigen.

- **Nach Beenden 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**.

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 des Programms von Kaspersky 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 anhalten, 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.

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.

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. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → 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.

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 Programme von Kaspersky aufgetreten sind. Die Informationen über Ereignisse werden in der Datenbank des Administrationsservers gespeichert.

Ereignisse nach Typ

In Kaspersky Security Center Linux gibt es die folgenden Ereignistypen:

- Allgemeine Ereignisse. Diese Ereignisse kommen in allen verwalteten Kaspersky-Programmen 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-Programme. Jedes verwaltete Kaspersky-Programm 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 Programmen generiert werden:

- Komponenten von Kaspersky Security Center Linux:
  - Administrationsserver
  - Administrationsagent
- Verwaltete Kaspersky-Programme

  Weitere Informationen zu den Ereignissen, die von verwalteten Kaspersky-Programmen generiert werden, finden Sie in der Dokumentation des entsprechenden Programms.

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 des Programms oder der 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 des Programms ohne Datenverlust oder eingeschränkter Funktionalität wiederhergestellt werden kann.
- *Infomeldung* – Ereignis, das zwecks Information über das erfolgreiche Ausführen einer Operation, die korrekte Ausführung des Programms 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 Datenbank des Administrationsservers gespeichert, da die für sie definierte Speicherdauer gleich Null ist. In externe Systeme können nur jene Ereignisse exportieren, die mindestens einen Tag in der Datenbank des Administrationsservers 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 Administrationsserver von Kaspersky Security Center und im Administrationsagenten auftreten können. Die Typen der Ereignisse, die in den Programmen von Kaspersky auftreten, sind in diesem Abschnitt nicht aufgeführt.

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.

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 Datenbank des Administrationsservers 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.

Ereignisse des Administrationsservers: Kritisch

Dargestellter Name	Ereignistyp-ID	Ereignistyp	Beschreibu

des Ereignistyps			
Lizenzbeschränkung wurde überschritten	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Kaspersky Security C überprüft einmal tägl Lizenzbeschränkung überschritten wurde. Ereignisse dieser Art wenn der Administrat erkennt, dass Beschr der Lizenz durch Kasp Anwendungen, die au Client-Geräten instal überschritten werden Außerdem tritt das E wenn die Anzahl der a genutzten Lizenzeinh von einer Lizenz abge werden, 110% der von abgedeckten Gesam Einheiten überschreit Auch wenn dieses Ere eintritt, werden die C Geräte geschützt. Sie können auf dieses folgendermaßen reag • Schauen Sie sich der verwalteten G Löschen Sie unge Geräte. • Stellen Sie eine Li weitere Geräte zu Verfügung (fügen Administrationsse gültigen Aktivieru oder eine Schlüss hinzu). Kaspersky Security C ermittelt die Regeln z Auslösen von Ereignis eine Lizenzbeschränk überschritten wurde.
Das Gerät wird nicht mehr verwaltet	4111	KLSRV_HOST_OUT_CONTROL	Ereignisse dieser Art wenn ein verwaltetes im Netzwerk sichtbar über einen bestimmte keine Verbindung zum Administrationsserve hergestellt hat.

			Finden Sie heraus, wa Administrationsagent diesem Gerät nicht ordnungsgemäß ausg wird. Mögliche Ursach Netzwerkprobleme o Entfernen des Administrationsagent diesem Gerät sein.
Gerätestatus - "Kritisch"	4113	KLSRV_HOST_STATUS_CRITICAL	Ereignisse dieser Art wenn einem verwalte der Status *Kritisch* zu wird. Sie können die Bedingungen anpass denen der Gerätesta *Kritisch* wechselt.
Die Schlüsseldatei wurde der Deny-Liste hinzugefügt	4124	KLSRV_LICENSE_BLACKLISTED	Ereignisse dieser Art wenn Kaspersky den verwendeten Aktivier oder die Schlüsselda Deny-Liste setzt. Kontaktieren Sie den Technischen Support Informationen.
Die Lizenz läuft bald ab	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Ereignisse dieser Art wenn das Ablaufdatu kommerziellen Lizenz rückt. Einmal am Tag überpr Kaspersky Security C Linux, ob sich das Ab der Lizenz nähert. Ve werden Ereignisse die 30 Tage, 15 Tage, 5 Ta Tag vor dem Ablaufd Lizenz. Die Anzahl de nicht geändert werde Administrationsserve entsprechenden Tag Ablaufdatum der Lize deaktiviert, so wird da erst am darauf folgen veröffentlicht. Wenn die kommerziel abläuft, stellt Kaspersky Security C nur grundlegende Fu bereit. Sie können auf dieses folgendermaßen reag • Vergewissern Sie dem Administratio ein Reserve-Lizen hinzugefügt wurd

			• Wenn Sie ein Abo verwenden, stelle dies zu Verlängerr unbeschränktes Abonnement wird automatisch verlä der vereinbarte B zum Fälligkeitsdat Dienstleister über wird.
Das Zertifikat ist abgelaufen	4132	KLSRV_CERTIFICATE_EXPIRED	Ereignisse dieser Art wenn das Zertifikat d Administrationsserve Funktion "Verwaltung Geräte" abläuft. Sie müssen das abge Zertifikat aktualisiere
Audit: Export nach SIEM fehlgeschlagen	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Ereignisse dieser Art wenn der Export von in das SIEM-System a eines Verbindungsfeh dem SIEM-System fehlgeschlagen ist.
Eingeschränkter Funktionsmodus	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Ereignisse dieser Art wenn Kaspersky Secu Linux beginnt, mit Grundlegenden Funk ohne Schwachstellen Patch-Management s Funktionalität "Mobile verwalten", zu arbeite Im Folgenden die Grü geeignete Reaktionen Ereignis: • Die Gültigkeitsdau Lizenz ist abgelau vollen Funktionsu Kaspersky Securit Linux zu nutzen, s eine Lizenz bereit dem Administratio einen gültigen Aktivierungscode Schlüsseldatei hin • Der Administratio verwaltet mehr Ge der Lizenz angege Verschieben Sie c aus der Administrationsgr Administrationsse eines anderen Administrationsse das Lizenzlimit de

			Administrationsse zulässt).
Updates der Programm-Module von Kaspersky wurden widerrufen	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Ereignisse dieser Art wenn nahtlose Updat Kaspersky-Experten zurückgerufen wurde Updates wird der Sta *Zurückgerufen* angez Beispiel, wenn Update neuere Version aktua werden müssen. Dies betrifft Patches für K Security Center Linu von Anwendungen, d Kaspersky verwaltet sind nicht betroffen. gibt den Grund an, wa nahtlose Update nich wurde.
Virenangriff	• 26 (für Schutz vor bedrohlichen Dateien) • 27 (für Schutz vor E-Mail-Bedrohungen) • 28 (für Firewall)	GNRL_EV_VIRUS_OUTBREAK	Ereignisse dieser Art wenn auf mehreren v Geräten die Anzahl a schädlichen Objekter Schwellwert innerhalb kurzen Zeitraums übe Sie können auf diese folgendermaßen reag • Legen Sie den Sch in den Eigenschaf Administrationsse • Erstellen Sie eine Richtlinie, die aktiv oder erstellen Sie Aufgabe, die bei A 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.

Ereignisse des Administrationsservers: Funktionsfehler

Dargestellter Name des	Ereignistyp-	Ereignistyp	Beschreibung

Ereignistyps	ID		
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.
Für eine der lizenzierten Programmgruppen wurde die Beschränkung für die Anzahl von Installationen überschritten	4126	KLSRV_INVLICPROD_EXCEDED	Der Administrationsserve generiert Ereignisse dieser Art periodisch (stündlich). Ereignisse dieser Art treten auf, wenn Sie in Kaspersky Security Center Linux die Lizenzschlüssel von Drittanbieter-Programmen verwalten und wenn die Anzahl der Installationen das Limit überschreitet, das durch den Lizenzschlüssel des Drittanbieter-Programms festgelegt ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Schauen Sie sich die Liste der verwalteten Geräte an. Löschen Sie Drittanbieter-Programme von den Geräten, auf denen si nicht verwendet werden. • Verwenden Sie eine Drittanbieter-Lizenz für mehr Geräte.

			Sie können die Lizenzschlüssel von Drittanbieter-Programmen verwalten, indem Sie die Funktionen der lizenzierten Programmgruppe verwenden. Zur lizenzierten Programmgruppe gehöre Drittanbieter-Programme, welche die von Ihnen festgelegten Kriterien erfüllen.
Kopieren der Updates in den angegebenen Ordner nicht ausgeführt	4123	KLSRV_UPD_REPL_FAIL	Ereignisse dieser Art treten auf, wenn Software-Updates in einen oder mehrere zusätzlich freigegebene Ordner kopiert werden. Sie können auf dieses Ereignis folgendermaßen reagieren: • Prüfen Sie, ob das Benutzerkonto, das fü den Zugriff auf die Ordner verwendet wird, über Berechtigung zum Schreiben verfügt. • Prüfen Sie, ob sich de Benutzername und/oder das Kennwort für den ode die Ordner geändert haben. • Überprüfen Sie die Internetverbindung, d sie die Ursache des Ereignisses sein kann. Folgen Sie den Anweisungen, um die Datenbanken und die Programm-Module zu aktualisieren.
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.

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 de Administrationsserve (auf dem sich der freigegebene Ordner befindet) angeschalte und erreichbar ist. • Prüfen Sie, ob sich de Benutzername und/oder das Kennwort zu diesem Ordner geändert haben. • Prüfen Sie die Netzwerkverbindung.
Die Administrationsserver-Datenbank ist nicht verfügbar	4109	KLSRV_DATABASE_UNAVAILABLE	Ereignisse dieser Art treten auf, wenn der Administrationsserver nicht verfügbar ist. Sie können auf dieses Ereignis folgendermaßen reagieren: • Prüfen Sie, ob der Remote-Server, auf dem SQL Server installiert ist, verfügba ist. • Schauen Sie in die Protokolle des DBMS, um die Ursache für die Nichtverfügbarkeit de Datenbank des Administrationsserve zu finden. Beispielsweise kann aufgrund von präventiven Wartungsarbeiten de Remote-Server, auf dem SQL Server installiert ist, nicht verfügbar sein.
Kein freier Platz in der Administrationsserver-	4110	KLSRV_DATABASE_FULL	Ereignisse dieser Art treten auf, wenn in der

Datenbank			Datenbank des Administrationsservers kein freier Speicherplatz mehr vorhanden ist. Der Administrationsserve funktioniert nicht, wenn seine Datenbank die Kapazitätsgrenze erreich 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 au dieses Ereignis: • Begrenzung der Anza der Ereignisse, die in der Datenbank des Administrationsserve gespeichert werden sollen. • In der Datenbank des Administrationsserve 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 Datenbank des Administrationsserve bezieht, ändern. Überprüfen Sie die Informationen zur Auswa des DBMS.
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 de Cloud-Umgebung durch den Administrationsserve fehlschlägt. Studieren Sie die Informationen in der Ereignisbeschreibung und

			reagieren Sie entsprechend.

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
Ein häufiges Ereignis wurde erkannt		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Ereignisse dieser Art treten auf, wenn der Administrationsserver häufiges auftretendes Ereignis auf einem verwalteten Gerät erkennt. Weitere Informationen finden S im folgenden Abschnit Blockieren von häufige Ereignissen.
Lizenzbeschränkung wurde überschritten	4098	KLSRV_EV_LICENSE_CHECK_100_110	Kaspersky Security Center Linux überprüf einmal täglich, ob eine Lizenzbeschränkung überschritten wurde. Ereignisse dieser Art treten auf, wenn der Administrationsserver erkennt, dass Beschränkungen der Lizenz durch Kaspersk Anwendungen, die auf den Client-Geräten installiert sind, überschritten werden. Außerdem tritt das Ereignis auf, wenn die Anzahl der aktuell genutzten Lizenzeinhe die von einer Lizenz abgedeckten werden, 100% bis 110% der von Lizenz abgedeckten Gesamtzahl an Einheit überschreitet.

			Auch wenn dieses Ere eintritt, werden die Cli Geräte geschützt. Sie können auf dieses Ereignis folgendermaß reagieren: • Schauen Sie sich d Liste der verwaltet Geräte an. Löscher Sie ungenutzte Geräte. • Stellen Sie eine Liz für weitere Geräte Verfügung (fügen S dem Administrationsser einen gültigen Aktivierungscode c eine Schlüsseldate hinzu). Kaspersky Security Center Linux ermittelt Regeln zum Auslösen v Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.
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 Fall, wenn ein verwalte Gerät ausrangiert wur Sie können auf dieses Ereignis folgendermaß reagieren: • Löschen Sie das G manuell aus der Lis der verwalteten Geräte. Geben Sie mithilfe Kaspersky Security Center Web Conso den Zeitraum an, na dessen Ablauf das Ereignis **Das Gerät war lange Zeit im Netzwerk inaktiv** erstellt wird. • Geben Sie mithilfe Kaspersky Security Center Web Conso den Zeitraum an, na

			dessen Ablauf das Gerät automatisch der Gruppe entfer wird.
Konflikt von Gerätenamen	4102	KLSRV_EVENT_HOSTS_CONFLICT	Ereignisse dieser Art treten auf, wenn der Administrationsserver zwei oder mehr verwal Geräte als ein Gerät wahrnimmt. Dies ist meistens dann Fall, wenn ein geklonte Laufwerk für die Bereitstellung auf verwalteten Geräten verwendet wurde, und dabei der Administrationsagent einem Referenzgerät r in den Modus für dezidierte Laufwerke geschaltet wurde. Um diesen Fehler zu vermeiden, schalten S den Administrationsagente auf einem Referenzge in den Modus zum Klor von Laufwerken, bevo das Laufwerk des Ger klonen.
Gerätestatus - "Warnung"	4114	KLSRV_HOST_STATUS_WARNING	Ereignisse dieser Art treten auf, wenn einen verwalteten Gerät der Status *Warnung* zugewiesen wird. Sie können die Bedingung anpassen, unter dener der Gerätestatus zu *Warnung* wechselt.
Für eine der lizenzierten Programmgruppen wird die Beschränkung für die Anzahl von Installationen bald überschritten	4127	KLSRV_INVLICPROD_FILLED	Ereignisse dieser Art treten auf, wenn die Anzahl der Installation von Dritthersteller-Programmen, die in eir lizenzierten Programmgruppe enthalten sein dürfen, 90% des in den Eigenschaften des Lizenzschlüssels angegeben zulässigen Werts erreicht. Sie können auf dieses Ereignis folgendermaß reagieren:

			• Wenn das Drittherstelle Programm auf einig verwalteten Geräte nicht verwendet wi löschen Sie das Programm von dies Geräten. • Wenn Sie erwarten dass die Anzahl de Installationen des Drittherstelle Programms das Maximum in nächst Zukunft übersteigt sollten Sie im Vorfe den Erwerb einer Drittherstelle-Lize für eine größere Anzahl an Geräten Erwägung ziehen. Sie können die Lizenzschlüssel von Drittanbieter-Programmen verwalte indem Sie die Funktion der lizenzierten Programmgruppe verwenden.
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 Ursachen für das Ereig und angebrachte Reaktionen darauf ausgeführt: • Die automatische Neuausstellung wu für ein Zertifikat initiiert, für das die Option **Zertifikat automatisch neu veröffentlichen, fa möglich** deaktivier Dies kann aufgrund eines Fehler geschehen, der bei Erstellung des Zertifikats auftrat. manuelles

			Neuausstellen des Zertifikats kann notwendig sein. • Wenn Sie eine Integration mit eine Public-Key-Infrastruktur verwenden, kann ei fehlendes Namensattribut de SAM-Benutzerkon welches für die PKI Integration und zur Ausstellen der Zertifikate genutzt wird, die Ursache s Überprüfen Sie die Eigenschaften des Benutzerkontos.
Zertifikat wurde entfernt	4134	KLSRV_CERTIFICATE_REMOVED	Ereignisse dieser Art treten auf, wenn ein Administrator ein Zertifikat beliebiger Ar (General, Mail, VPN) fü die Funktion "Verwaltu mobiler Geräte" entfer Nach dem Entfernen eines Zertifikats schläg für die mobilen Geräte über dieses Zertifikat verbunden sind, die Verbindung mit dem Administrationsserver fehl. Dieses Ereignis kann hilfreich sein, wenn es darum geht, Fehlfunktionen im Zusammenhang mit de Verwaltung mobiler Geräte aufzuspüren.
Das APNs-Zertifikat ist abgelaufen	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Ereignisse dieser Art treten auf, wenn ein APNs-Zertifikat abläuf Sie müssen manuell da APNs-Zertifikat erneu und es auf einem iOS MDM-Server installiere
Das APNs-Zertifikat läuft bald ab	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Ereignisse dieser Art treten auf, wenn das APNs-Zertifikat in wer als 14 Tagen abläuft.

			Wenn das APNs-Zerti abläuft, müssen Sie manuell das APNs-Zertifikat erneuern und auf einem iOS MDM-Server installieren. Es wird empfohlen, das Sie den Zeitpunkt für d Erneuern des APNs-Zertifikats vor das Ablaufdatum legen.
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 si Google Firebase Cloud Messaging (FCM) für d Verbindung verwaltete Geräte mit Android-Betriebssystem verwendet, und auf de FCM-Server das Bearbeiten von empfangenen Administrationsserver Anfragen fehlschlägt. bedeutet, dass einige verwalteten mobilen Geräte keine PUSH-Benachrichtigungen empfangen. Studieren Sie den HTT Code in den Details de Ereignisbeschreibung reagieren Sie entsprechend. Weitere Informationen über HT Codes, die vom FCM-Server empfangen wurden, und damit verbundene Fehler, entnehmen Sie bitte d Dokumentation von Google Firebase Servi (siehe Kapitel "Antwortcodes für nachgeschaltete Nachrichtenfehler").
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 si Google Firebase Cloud Messaging (FCM) für d Verbindung verwaltete Geräte mit Android-

			Betriebssystem verwendet, und der FC Server auf eine Administrationsserver Anfrage einen anderer HTTP-Code als 200 (" zurück zurückgibt. Im Folgenden werden Ursachen für das Ereig und angebrachte Reaktionen darauf ausgeführt: • Probleme mit dem FCM-Server. Studieren Sie den HTTP-Code in den Details der Ereignisbeschreibu und reagieren Sie entsprechend. Wei Informationen über HTTP-Codes, die v FCM-Server empfangen wurder und damit verbund Fehler, entnehmen bitte der Dokumentation vo Google Firebase Service (siehe Kapi "Antwortcodes für nachgeschaltete Nachrichtenfehler" • Probleme mit dem Proxyserver (wenn einen Proxyserver benutzen). Studier Sie den HTTP-Cod den Details des Ereignisses und reagieren Sie entsprechend.
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 Verwendu des Google Firebase Cloud Messaging HTT Protokolls unerwartete Fehler auf dem Administrationsserver auftreten. Studieren Sie die Informationen in der Ereignisbeschreibung reagieren Sie entsprechend.

			Wenn Sie selbst keine Lösung für dieses Problem ausmachen können, ist es empfehlenswert den Technischen Support Kaspersky zu kontaktieren.
Auf der Festplatte ist wenig freier Platz vorhanden	4105	KLSRV_NO_SPACE_ON_VOLUMES	Ereignisse dieser Art treten auf, wenn auf d Gerät, auf dem der Administrationsserver installiert ist, der Speicherplatz knapp w Schaffen Sie freien Speicherplatz.
Wenig freier Platz in der Administrationsserver-Datenbank	4106	KLSRV_NO_SPACE_IN_DATABASE	Ereignisse dieser Art treten auf, wenn der P in der Datenbank des Administrationsserver knapp ist. Wenn Sie di Situation nicht lösen, erreicht die Datenbanl des Administrationsserver bald ihre Kapazitätsgr und der Administrationsserver wird nicht länger funktionieren. Nachfolgend finden Si die Ursachen für diese Ereignis in Abhängigke vom DBMS, das Sie verwenden, sowie geeignete Reaktionen dieses Ereignis. • Begrenzen Sie nich die Anzahl der Ereignisse, die in de Datenbank des Administrationsser gespeichert werde sollen. • Reduzieren Sie die Liste an Ereignisse die in der Datenbar des Administrationsser gespeichert werde sollen. Überprüfen Sie die Informationen zur Aus des DBMS.

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-Protc des Geräts, auf dem d sekundäre Administrationsserver installiert ist, und reagieren Sie entsprechend.
Die Verbindung mit dem primären Administrationsserver wurde getrennt	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Ereignisse dieser Art treten auf, wenn die Verbindung zum primä Administrationsserver unterbrochen ist. Konsultieren Sie das Betriebssystem-Protc des Geräts, auf dem d primäre Administrationsserver installiert ist, und reagieren Sie entsprechend.
Neue Updates der Programm-Module von Kaspersky sind registriert	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Ereignisse dieser Art treten auf, wenn der Administrationsserver Kaspersky-Software, auf verwalteten Gerät installiert ist, neue Updates registriert, welche eine Genehmig für die Installation benötigen. Sie können diese Upda in der Kaspersky Secu Center Web Console genehmigen oder ablehnen.
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 Ereigr aus der Datenbank des Administrationsserver begonnen hat, nachde die Kapazitätsgrenze d Datenbank des Administrationsserver erreicht wurde. Sie können auf dieses Ereignis folgendermaß reagieren:

			• Ändern Sie die maximale Anzahl vo Ereignissen, die in d Datenbank des Administrationsser gespeichert sind. • Reduzieren Sie die Liste an Ereignisse die in der Datenbar des Administrationsser gespeichert werde sollen.
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 Datenbank des Administrationsserver gelöscht wurden, nachdem die Kapazitätsgrenze der Datenbank des Administrationsserver erreicht wurde. Sie können auf dieses Ereignis folgendermaß reagieren: • Ändern Sie die zulässige maximale Anzahl von Ereignissen, die in d Datenbank des Administrationsser gespeichert sind. • Reduzieren Sie die Liste an Ereignisse die in der Datenbar des Administrationsser gespeichert werde sollen.
Audit: (testweise Verbindung zu SIEM-Server fehlgeschlagen)	5120	KLAUD_EV_SIEM_TEST_FAILED	Ereignisse dieser Art treten auf, wenn ein automatischer Verbindungstest mit d SIEM-Server fehlgeschlagen ist.

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
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 abgedeckte werden, mehr als 90% d von der Lizenz abgedeckten Gesamtza an Einheiten überschreitet. Die Client-Geräte sind selbst dann geschützt, wenn eine Lizenzbeschränkung überschritten wird. Sie können auf dieses Ereignis folgendermaße reagieren: • Schauen Sie sich die Liste der verwaltete Geräte an. Löschen Sie ungenutzte Geräte. • Stellen Sie eine Lizer für weitere Geräte z Verfügung (fügen Si dem Administrationsserv einen gültigen Aktivierungscode oc eine Schlüsseldatei hinzu).

			Kaspersky Security Center Linux ermittelt d Regeln zum Auslösen vo Ereignissen, wenn eine Lizenzbeschränkung überschritten wurde.
Neues Gerät wurde erkannt	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	Ereignisse dieser Art treten auf, wenn im Netzwerk neue Geräte entdeckt wurden.
Gerät wurde automatisch zur Gruppe hinzugefügt	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	Ereignisse dieser Art treten auf, wenn Geräte gemäß den Regeln für d Verschieben von Geräte einer Gruppe zugewiese wurden.
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 wurde
Die Beschränkung für die Anzahl von Installationen wird für eine der lizenzierten Programmgruppen bald überschritten (mehr als 95% verbraucht)	4128	KLSRV_INVLICPROD_EXPIRED_SOON	Ereignisse dieser Art treten auf, wenn die Anzahl der Installationer von Drittherstеller-Programmen, die in eine lizenzierten Programmgruppe enthalten sein dürfen, 90% des in den Eigenschaften des Lizenzschlüssels angegeben zulässigen Werts erreicht. Sie können auf dieses Ereignis folgendermaße reagieren: • Wenn das Drittherstеller-Programm auf einige verwalteten Geräter nicht verwendet wird löschen Sie das Programm von diese Geräten. • Wenn Sie erwarten, dass die Anzahl der Installationen des Drittherstеller-Programms das Maximum in nächste Zukunft übersteigt, sollten Sie im Vorfeld den Erwerb einer Drittherstеller-Lizen

			für eine größere Anzahl an Geräten in Erwägung ziehen. Sie können die Lizenzschlüssel von Drittanbieter-Programmen verwalten, indem Sie die Funktione der lizenzierten Programmgruppe verwenden.
Die ID der FCM Instance hat sich auf diesem mobilen Gerät geändert	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	Ereignisse dieser Art treten auf, wenn sich de Token von Firebase Clou Messaging auf dem Ger geändert hat. Informationen zur Rotation des FCM-Tokens finden Sie in der Dokumentation des Firebase-Dienstes.
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 Administrationsserver** das Kopieren der Dateie in den angegebenen Ordner abgeschlossen hat.
Die Verbindung mit dem sekundären Administrationsserver wurde hergestellt	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	Weitere Informationen dazu finden Sie in diese Thema: Hierarchie der Administrationsserver erstellen: einen sekundären Administrationsserver hinzufügen.
Die Verbindung mit dem primären Administrationsserver wurde hergestellt	4117	KLSRV_EV_MASTER_SRV_CONNECTED	
Datenbanken wurden aktualisiert	4144	KLSRV_UPD_BASES_UPDATED	Ereignisse dieser Art treten ein, wenn die Aufgabe **Download von Updates in die Datenverwaltung des Administrationsserver** das Aktualisieren der Datenbanken abgeschlossen hat.
Audit: Verbindung mit dem	4147	KLAUD_EV_SERVERCONNECT	

Administrationsserver wurde hergestellt			
Audit: Objekt wurde modifiziert	4148	KLAUD_EV_OBJECTMODIFY	Dieses Ereignis verfolgt Änderungen in den folgenden Objekten: • Administrationsgrup • Sicherheitsgruppe • Benutzer • Paket • Aufgabe • Richtlinie • Server • Virtueller Server
Audit: Objektstatus wurde geändert	4150	KLAUD_EV_TASK_STATE_CHANGED	Dieses Ereignis tritt beispielsweise auf, wenn eine Aufgabe mit einem Fehler beendet wurde.
Audit: Gruppeneinstellungen wurden modifiziert	4149	KLAUD_EV_ADMGROUP_CHANGED	Ereignisse dieser Art treten auf, wenn eine Sicherheitsgruppe bearbeitet wurde:
Audit: Die Verbindung mit dem Administrationsserver wurde unterbrochen	4151	KLAUD_EV_SERVERDISCONNECT	
Audit: Objekteigenschaften wurden geändert	4152	KLAUD_EV_OBJECTPROPMODIFIED	Dieses Ereignis verfolgt Änderungen der folgenden Eigenschafte • Benutzer • Lizenz • Server • Virtueller Server
Audit: Benutzerrechte wurden geändert	4153	KLAUD_EV_OBJECTACLMODIFIED	
Audit: Die Chiffrierschlüssel wurden vom Administrationsserver importiert oder exportiert	5100	KLAUD_EV_DPEKEYSEXPORT	Dieses Ereignis tritt beispielsweise während der Migration auf.

Audit: (testweise Verbindung zu SIEM-Server erfolgreich)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	Ereignisse dieser Art treten auf, wenn eine testweise Verbindung m dem SIEM-Server erfolgreich war.
Es wurden Dateien gefunden, die zur Analyse an Kaspersky gesendet werden	4131	KLSRV_APS_FILE_APPEARED	

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

Dargestellter Name des Ereignistyps	Ereignistyp-ID	Ereignistyp	Beschreibung
Fehler bei der Update-Installation	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn das Automatische Update und das Patchen von Komponenten von Kaspersky Security Center Linux nicht erfolgreich waren. Das Ereignis betrifft nicht die Updates von verwalteten Kaspersky-Programmen.

			Lesen Sie die Ereignisbeschreibung. Ein Windows-Problem auf dem Administrationsserver kann ein Grund für dieses Ereignis sein. Wenn die Beschreibung ein Problem in der Windows-Konfiguration erwähnt, beheben Sie dieses.
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 das Update einer Drittanbieter-Software nicht erfolgreich war. Überprüfen Sie, ob der Link zur Software für Drittanbieter gültig ist. Lesen Sie die Ereignisbeschreibung.
Installation der Updates von Windows-Update fehlgeschlagen	7717	KLNAG_EV_WUA_INSTALL_ERROR	Ereignisse dieser Art treten auf, wenn Windows Updates nicht erfolgreich waren. Lesen Sie die Ereignisbeschreibung. Suchen Sie nach dem Fehler in der Microsoft Knowledge Base. Wenden Sie sich an den technischen Support von Microsoft, wenn Sie das Problem nicht selbst lösen können.

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
Es ist ein Sicherheitsproblem aufgetreten	549	GNRL_EV_APP_INCIDENT_OCCURED	Ereignisse dieser Art treten auf, wenn auf einem Gerät ein Vorfa gefunden wurde . Dies Ereignis tritt beispielsweise auf, wer auf dem Gerät nur noc wenig Speicherplatz verfügbar ist.
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 d konfigurierte KSN-Pro Verbindung fehlschläg
Installation des Updates für Drittherstellersoftware wurde aufgeschoben	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Ereignisse dieser Art treten beispielsweise a wenn die EULA für die Installation eines Drittanbieter-Updates abgelehnt wird.
Installation des Updates für die Drittherstellersoftware wurde mit einer Warnung abgeschlossen	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Laden Sie die Ablaufverfolgungsdat herunter und überprüf Sie den Wert des Feld KLRI_PATCH_RES_DE auf Details.
Während der Installation des Updates des Software-Moduls wurde eine Warnung zurückgegeben	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Laden Sie die Ablaufverfolgungsdat herunter und überprüf Sie den Wert des Feld KLRI_PATCH_RES_DE auf Details.

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	Standar Speicherd
Programm wurde installiert	7703	KLNAG_EV_INV_APP_INSTALLED	30 Tage
Programm wurde deinstalliert	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 Tage

Überwachtes Programm wurde installiert	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 Tage
Überwachtes Programm wurde deinstalliert	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 Tage
Neues Gerät wurde hinzugefügt	7708	KLNAG_EV_DEVICE_ARRIVAL	30 Tage
Gerät wurde entfernt	7709	KLNAG_EV_DEVICE_REMOVE	30 Tage
Neues Gerät wurde erkannt	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 Tage
Gerät wurde autorisiert	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	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
Drittherstellerprogramm 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
Installation des Updates des Software-Moduls wurde gestartet	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 Tage
Windows Desktopfreigabe: Das Programm 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:	7716	KLUSRLOG_EV_WDS_END	30 Tage

Beendet			

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 und Berichterstattung** unter **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 der verwalteten Programme)
- **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 Datenbank des Administrationsservers löschen

Ereignisauswahl erstellen

Um eine Ereignisauswahl zu erstellen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **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.
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 Auswahlergebnis wechseln** aktiviert.
6. Klicken Sie auf **Speichern**, um die Erstellung der Ereignisauswahl zu bestätigen.

Wenn Sie das Kontrollkästchen **Zum Auswahlergebnis 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 und Berichterstattung** → **Ereignisauswahlen**.
2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie bearbeiten möchten.
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. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → Ereignisauswahlen**.
2. Aktivieren Sie das Kontrollkästchen neben der Ereignisauswahl, die Sie starten möchten.
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 für Ereignisauswahl anpassen** die Einstellungen für die Sortierung an.
     c. 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.

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 und Berichterstattung → 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 und Berichterstattung → 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 erfolgreichem 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.
3. Im angezeigten Fenster können Sie Folgendes tun:

   - Informationen zum ausgewählten Ereignis ansehen
   - Das nächste und vorige Ereignis im Ergebnis der Ereignisauswahl öffnen

- 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

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.
3. Klicken Sie auf die Schaltfläche **In Datei exportieren**.

Das ausgewählte Ereignis wird in eine 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

Um eine oder mehrere Ereignisse zu löschen, gehen Sie wie folgt vor:

1. Starten einer Ereignisauswahl.
2. Aktivieren Sie die Kontrollkästchen neben den gewünschten Ereignissen.
3. Klicken Sie auf die Schaltfläche **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 und Berichterstattung** → **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 Programme von Kaspersky aufgetreten sind. Die Informationen über Ereignisse werden in der Datenbank des Administrationsservers gespeichert. Möglicherweise sollen bestimmte Ereignisse länger oder kürzer aufbewahrt werden, als durch die Standardwerte festgelegt. 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 Datenbank des Administrationsservers fest:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Führen Sie eine der folgenden Aktionen aus:

   - Um die Speicherdauer für die Ereignisse des Administrationsagenten oder eines verwalteten Kaspersky-Programms anzupassen, klicken Sie auf den Namen der entsprechenden Richtlinie.

     Die Eigenschaftenseite der Richtlinie wird geöffnet.

   - Um die Administrationsserver-Ereignisse anzupassen, klicken Sie im Hauptmenü auf das Einstellungen-Symbol () neben dem Namen des entsprechenden Administrationsservers.

     Wenn Sie eine Richtlinie für den Administrationsserver haben, können Sie stattdessen auf den Namen dieser Richtlinie klicken.

Die Eigenschaftenseite des Administrationsservers (oder die Eigenschaftenseite der Administrationsserver-Richtlinie) wird geöffnet.

3. Wählen Sie die Registerkarte **Konfiguration von Ereignissen** aus.

   Eine Liste der Ereignistypen, die sich auf den Abschnitt **Kritisch** beziehen, wird angezeigt.

4. Wählen Sie **Funktionsfehler**, **Warnung** oder **Information** aus.

5. 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 die Option **In der Administrationsserver-Datenbank speichern für (Tage)** aktiviert.

6. Geben Sie im Bearbeitungsfeld unterhalb dieser Umschalttaste die Anzahl der Tage ein, über die das Ereignis gespeichert werden soll.

7. 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.

8. Klicken Sie auf die Schaltfläche **OK**.

   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

Ein verwaltetes Programm (z. B. Kaspersky Endpoint Security für Linux), das 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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 die Blockade 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 dadurch solange empfangen, bis der Administrationsserver diese häufig auftretenden Ereignissen erneut blockiert.

Um die Blockade für häufig auftretende Ereignisse aufzuheben:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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 über die Ausführung des Programms und der verwalteten Geräte werden in der Datenbank des Administrationsservers 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 vom Programm 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 Datenbank des Servers 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 Datenbank des Administrationsservers 400.000 Ereignisse. Die empfohlene Maximalgröße der Datenbank liegt bei 45 Millionen Ereignissen.

Das Programm überprüft die Datenbank alle 10 Minuten. Wenn die Anzahl der Ereignisse den festgelegten Höchstwert plus 10.000 erreicht, löscht das Programm 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 dieser Zeitspanne 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.

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 und Berichterstattung → 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 und Berichterstattung → 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. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → Benachrichtigungen**.

   Im linken Bereich ist die Kategorie **Alle Benachrichtigungen** ausgewählt, und im rechten Bereich werden alle Benachrichtigungen angezeigt.

2. Wählen Sie im linken Bereich eine der drei Kategorien:

   - **Bereitstellung**
   - **Geräte**
   - **Schutz**
   - **Updates** (Diese Kategorie umfasst Benachrichtigungen über Programme von Kaspersky, die zum Download verfügbar sind und Benachrichtigungen über Updates der Antiviren-Datenbanken, die heruntergeladen wurden.)
   - **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.)
   - **Neuigkeiten von Kaspersky** (Diese Kategorie enthält Informationen über Veröffentlichungen von Kaspersky-Programmen.)

   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**. 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 **Web-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 und Berichterstattung**.

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 in bestimmten Fällen das Sichtbarkeits-Flag des Gerätes im Netzwerk berücksichtigt (siehe folgende Tabelle). 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
Es wurde keine Sicherheitsanwendung 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-	Über 0.

	Untersuchung) mehrere Viren gefunden, und die Anzahl der gefundenen Viren übersteigt den angegebenen Wert.	
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 Datenbank des Administrationsservers 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 Datenbank des Administrationsservers 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 werden erkannt	Die Anzahl der unbearbeiteten Objekte im Ordner **Aktive Bedrohungen** übersteigt den angegebenen Wert.	Über 0 Elemente.
Neustart erforderlich	Das Gerät ist im Netzwerk sichtbar, aber ein Programm erfordert aufgrund einer der angegeben Bedingungen einen Neustart des Gerätes, der nicht innerhalb des festgelegten Zeitraums ausgeführt wurde.	Über 0 Minuten.
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 Programme 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.
Die letzte Suche nach Windows-Updates liegt lange zurück	Das Gerät ist im Netzwerk sichtbar, aber die Aufgabe *Windows-Updates synchronisieren* 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 Verwaltungsprogrammen von Kaspersky als auch manuell durch den Administrator erstellt werden.	• Umschalter deaktiviert. • Umschalter aktiviert.
Gerätestatus wird vom	Der Gerätestatus wird vom verwalteten Programm	• Umschalter deaktiviert.

Programm bestimmt	bestimmt.	• Umschalter 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 Kaspersky Security Center Linux von der vorhergehenden Version upgraden, bleiben die Werte für die Zuweisung der Statusvarianten *Kritisch* oder *Warnung* für die Bedingung **Die Datenbanken sind veraltet** unverändert.

Wenn Kaspersky Security Center Linux einem Gerät einen Status zuweist, wird für bestimmte Bedingungen (siehe Spalte "Beschreibung der Bedingung" in der obigen Tabelle) das Sichtbarkeits-Flag berücksichtigt. 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*.

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 **Assets (Geräte)** → **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 **Kritisch** aus.
5. Aktivieren Sie im rechten Bereich im Abschnitt **Werte, für die der Status auf "Kritisch" gesetzt wird** 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 **Assets (Geräte)** → **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 **Werte, für die der Status auf "Warnung" gesetzt wird** 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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:

- **TLS nicht 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: Das Programm 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 die das Programm 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, die das Programm 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:

- **TLS nicht 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: Das Programm sendet dann 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, die das Programm während des angegebenen Zeitintervalls versenden darf.

- **Start einer ausführbaren Datei**

  Wenn diese Methode der Zustellung von Benachrichtigungen ausgewählt ist, können Sie im Eingabefeld das Programm angeben, das 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.

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 des Programms 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 das Programm 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. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **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 Sicherheits-Apps 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 Parameterplatzhaltern für das Ereignis enthalten, die dem Administrator übermittelt werden müssen.

Parameterplatzhalter zur Beschreibung des Ereignisses

Parameterplatzhalter	Beschreibung des Parameterplatzhalters
%SEVERITY%	Ereigniskategorie
%COMPUTER%	Name des Geräts, auf dem das Ereignis eingetreten ist
%DOMAIN%	Domäne
%EVENT%	Ereignis
%DESCR%	Ereignisbeschreibung
%RISE_TIME%	Zeitpunkt des Auftretens
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Aufgabenname
%KL_PRODUCT%	Administrationsagent
%KL_VERSION%	Versionsnummer des Administrationsagenten
%HOST_IP%	IP-Adresse
%HOST_CONN_IP%	IP-Adresse der Verbindung

Beispiel:

Ausführbare Datei zur Benachrichtigung über Ereignisse (z. B. script1.bat), innerhalb der eine weitere ausführbare Datei (z. B. script2.bat) mit dem Parameterplatzhalter %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 dem Parameter %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 und Berichterstattung → Mitteilungen von Kaspersky**) finden Sie Wissenswertes zu Ihrer Version von Kaspersky Security Center Linux und den verwalteten Programmen, 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-Programme 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-Programme auf dem neuesten Stand und voll funktionsfähig gehalten. Die Mitteilungen können Informationen über kritische Updates für Kaspersky-Programme, Korrekturen für gefundene Schwachstellen und Methoden zum Beheben sonstiger Probleme in Kaspersky-Programmen 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-Programme 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-Programme, 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. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung → 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 Berichterstattung** 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 und Berichterstattung → Mitteilungen von Kaspersky**) finden Sie Wissenswertes zu Ihrer Version von Kaspersky Security Center Linux und den verwalteten Programmen, 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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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.

Stellen Sie sicher, dass Sie einen Lizenzschlüssel für EDR Optimum hinzufügen , um Informationen über erkannte Bedrohungen auf den Endgeräten anzuzeigen.

*So aktivieren oder deaktivieren Sie die Anzeige von Abschnitt **Alarme** im Hauptmenü:*

1. Wechseln Sie im Hauptmenü zu Ihren Kontoeinstellungen und wählen Sie anschließend **Einstellungen der Benutzeroberfläche.**

2. Aktivieren oder deaktivieren Sie die Option **Alarme von EDR anzeigen**.

3. Klicken Sie auf **Speichern**.

Wenn diese Option aktiviert ist, zeigt die Konsole den Unterabschnitt **Alarme** im Abschnitt **Überwachung und Berichterstattung** des Hauptmenüs an. Im Unterabschnitt **Alarme** können Sie Informationen über die Erkennung von Bedrohungen auf den Endpunktgeräten anzeigen. Sie können auch ein Widget hinzufügen, welches Informationen zu Warnungen anzeigt. Wenn Sie das Plug-in von EDR Optimum installiert haben, können Sie außerdem detaillierte Informationen zu erkannten Bedrohungen anzeigen, indem Sie auf den Link **mehr Details** klicken.

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
- anderes Programm
- 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

Cloud Discovery

Kaspersky Security Center Linux ermöglicht es Ihnen, die Verwendung von Cloud-Diensten auf verwalteten Windows-Geräten zu überwachen und den Zugriff auf unerwünschte Cloud-Dienste zu blockieren.
Cloud Discovery überwacht die Zugriffsversuche von Benutzern auf diese Dienste sowohl über Browser als auch über Desktop-Anwendungen. Es überwacht obendrein die Versuche von Benutzern, über unverschlüsselte Verbindungen (z. B. mittels HTTP-Protokolls) Zugriff auf Cloud-Dienste zu erhalten. Diese Funktion hilft Ihnen, die Verwendung von Cloud-Diensten durch Schatten-IT zu erkennen und zu stoppen.

Die Funktion zum Blockieren ist nur verfügbar, wenn Sie Kaspersky Security Center Linux unter einer Lizenz für Kaspersky Security Center Linux EDR Optimum oder 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 sollen.

Um den Zugriff auf unerwünschte Cloud-Dienste blockieren zu können, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- 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 Widget und die Berichte von Cloud Discovery zeigen Informationen über erfolgreiche und blockierte Zugriffsversuche auf Cloud-Dienste an. Das Widget zeigt auch für jeden Cloud-Dienst die Risikostufe an. Kaspersky Security Center Linux ruft die Informationen zur Verwendung von Cloud-Diensten von all den 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 all den 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 Widgets von Cloud Discovery.
- 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 im Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen** über die Berechtigung **Schreiben** verfügen.

So aktivieren Sie die Cloud Discovery-Funktion mithilfe des Widgets von Cloud Discovery:

1. Wechseln Sie zu Kaspersky Security Center Linux.
2. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
3. Klicken Sie im Widget **Cloud Discovery** auf die Schaltfläche **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 die Schaltfläche **Aktivieren**.

   Die folgenden Richtlinieneinstellungen werden dabei 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.

Widget von Cloud Discovery zum Dashboard hinzufügen

Sie können das Widget von **Cloud Discovery** zum Dashboard hinzufügen, um die Nutzung von Cloud-Diensten auf verwalteten Geräten zu überwachen.

Um das Widget von Cloud Discovery zum Dashboard hinzuzufügen, müssen Sie im Funktionsbereich **Allgemeine Funktionen: Grundlegende Funktionen** über die Berechtigung **Schreiben** verfügen.

So fügen Sie das Widget von Cloud Discovery zum Dashboard hinzu:

1. Wechseln Sie zu Kaspersky Security Center Linux.
2. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.
3. Klicken Sie auf die Schaltfläche **Web-Widget hinzufügen oder wiederherstellen**.
4. Klicken Sie in der Liste der verfügbaren Widgets auf das Pfeilsymbol (>) neben der Kategorie **Andere**.
5. Wählen Sie das Widget **Cloud Discovery** aus und klicken Sie anschließend auf die Schaltfläche **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 Widget **Cloud Discovery** anzeigen, das Informationen zu versuchten Zugriffen auf Cloud-Dienste zur Verfügung stellt. Das Widget zeigt auch für jeden Cloud-Dienst die Risikostufe an. Kaspersky Security Center Linux ruft die Informationen zur Verwendung von Cloud-Diensten von all den verwalteten Geräten ab, die nur durch jene Sicherheitsprofile geschützt sind, für welche die Funktion aktiviert ist.

Stellen Sie vor dem Anzeigen sicher, dass:

- das Widget von Cloud Discovery dem Dashboard hinzugefügt wurde.
- die Cloud Discovery-Funktion ist aktiviert.
- Sie über die Berechtigungen **Lesen** in dem Funktionsbereich Lesen: **Grundlegende Funktionen** verfügen.

So zeigen Sie das Widget "Cloud Discovery" an:

1. Wechseln Sie zu Kaspersky Security Center Linux.
2. Wechseln Sie im Hauptmenü zu **Überwachung und Berichterstattung** → **Dashboard**.

   Das Widget **Cloud Discovery** wird auf dem Dashboard angezeigt.
3. Wählen Sie auf der linken Seite des Widgets **Cloud Discovery** eine Kategorie von Cloud-Diensten.

   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.

   In der unteren Tabelle sind bis zu zehn Geräte enthalten, die am häufigsten versuchen, auf den Dienst zuzugreifen.

Das Widget zeigt die angeforderten Informationen an.

Im angezeigten Widget können Sie:

- Zum Abschnitt **Überwachung und Berichterstattung** → **Berichte** wechseln, um die Berichte von Cloud Discovery anzuzeigen.
- Für den ausgewählten Cloud-Dienst den Zugriff blockieren oder erlauben.

Die Funktion zum Blockieren ist nur verfügbar, wenn Sie Kaspersky Security Center Linux unter einer Lizenz für Kaspersky Security Center Linux EDR Optimum oder 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

Für jeden Cloud-Dienst zeigt Cloud Discovery Ihnen eine Risikostufe an. Die Risikostufe hilft Ihnen beim Identifizieren von Cloud-Diensten, 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 Anbieter des Dienstes aussagt. Die Risikostufe stellt lediglich eine Empfehlung von Kaspersky-Experten dar.

Die Risikostufen der Cloud-Dienste werden im Widget von Cloud Discovery 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 muss, sollten 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 nacheinander sperren.

- In den Eigenschaften der Richtlinie von Kaspersky Endpoint Security für Windows.

  In diesem Fall können Sie den Zugriff auf die Dienste nacheinander oder für eine komplette Kategorie auf einmal 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 in dem Bereich **Top 10 der Geräte, die diesen Dienst verwenden**, nach der Sicherheitsrichtlinie oder dem Profil, für die bzw. für das Sie den Dienst blockieren oder zulassen möchten.
3. Führen Sie in der erforderlichen 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 die Schaltfläche **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.

Szenario: Ereignisexport in SIEM-Systeme konfigurieren

Kaspersky Security Center Linux ermöglicht die Konfiguration des Ereignisexports in SIEM-Systeme. Dafür gibt es folgende Methoden: Export in ein beliebiges SIEM-System, das das Syslog-Format verwendet, oder Export von Ereignissen in SIEM-Systeme direkt aus der Kaspersky Security Center-Datenbank. 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-Apps auftreten. Dann können Sie die Ereignisse für bestimmte verwaltete Kaspersky-Apps markieren.

- **Konfigurieren des Exports von Ereignissen in das SIEM-System**

  Der Export von Ereignissen kann auf folgende Weisen erfolgen:

  - Mittels der Protokolle TCP/IP, 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 Programme von Kaspersky aufgetreten sind. Die Informationen über Ereignisse werden in der Datenbank des Administrationsservers 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 Apps im Echtzeitbetrieb gewährleisten, sowie Security Operation Center (SOC).

Diese Systeme erhalten Daten aus vielen Quellen, einschließlich Netzwerke, Sicherheitssysteme, Server, Datenbanken und Apps. 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.

Syslog-Format des Ereignisexports

Sie können Ereignisse im Syslog-Format an ein beliebiges SIEM-System senden. Mit dem Syslog-Format können beliebige Ereignisse übertragen werden, die auf dem Administrationsserver und in Kaspersky-Apps, auf verwalteten Geräten installiert sind, auftreten. Beim Exportieren von Ereignissen im Syslog-Format können Sie genau festlegen, welche Arten von Ereignissen an das SIEM-System übertragen 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**

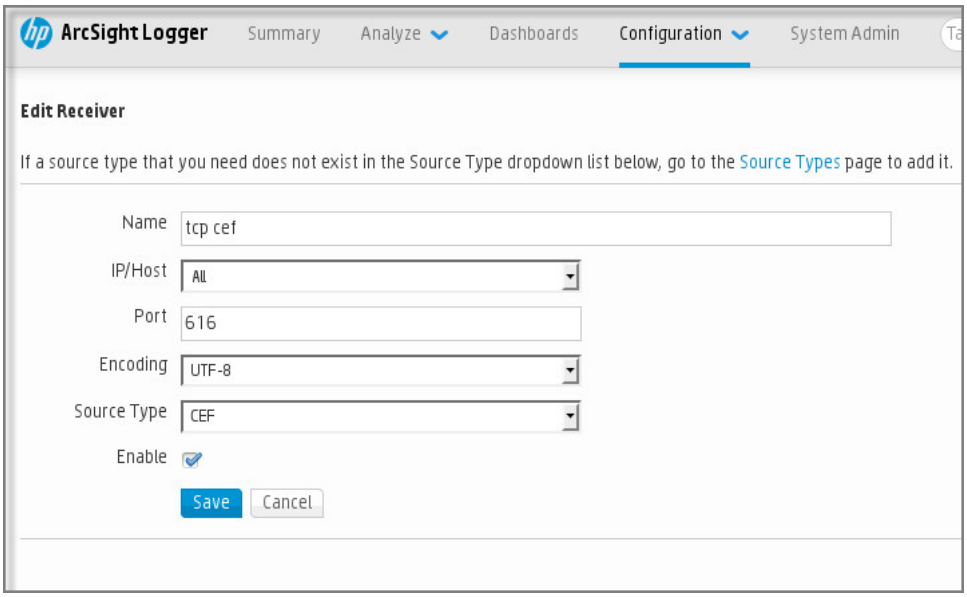
  Geben Sie die Portnummer für die Verbindung mit Kaspersky Security Center Linux an. Dieser Port muss derselbe sein wie der Port, den Sie in Kaspersky Security Center Linux bei der Konfiguration für das SIEM-System angeben.

- **Datenformat**

  Geben Sie das Syslog-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; sie werden für die Aufteilung der Nachrichten in Felder, etwa ID der Nachricht, Signifikanz, Beschreibung und die übrigen Einstellungen 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.

Ereignisse zum Export in SIEM-Systeme im Syslog-Format markieren

Dieser Abschnitt beschreibt das Auswählen von Ereignissen für den weiteren Export in SIEM-Systeme mittels Syslog-Format.

Über das Markieren von Ereignissen zum Export in SIEM-Systeme im Syslog-Format

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 Programmen auftreten, die von der Richtlinie verwaltet werden. Falls die zu

exportierenden Ereignisse in der Richtlinie ausgewählt worden sind, ist es unmöglich, diese für ein einzelnes Programm, das von dieser Richtlinie verwaltet wird, umzudefinieren.

- Ereignisse für ein verwaltetes Programm markieren. Wenn Sie die zu exportierenden Ereignisse für ein verwaltetes Programm auf einem verwalteten Gerät markieren, werden nur Ereignisse in das SIEM-System übertragen, die in diesem Programm aufgetreten sind.

Ereignisse von Kaspersky-Programmen zum Export im Syslog-Format markieren

Wenn Sie Ereignisse exportieren möchten, die in einem bestimmten verwalteten Programm, welches auf den verwalteten Geräten installiert ist, auftreten, markieren Sie in der Programmrichtlinie 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 ein bestimmtes verwaltetes Programm zu markieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie des Programms, für welches Sie die Ereignisse markieren möchten.

   Das Fenster mit den Richtlinieneinstellungen wird geöffnet.
3. Wechseln 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 dem verwalteten Programm 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 Programmrichtlinie 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 **Assets (Geräte)** → **Verwaltete 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. Wechseln Sie zum Abschnitt **Programme**.
4. Klicken Sie in der Liste der Programme auf den Link mit dem Namen des benötigten Programms.
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 eine der folgenden Aktionen aus:
   - Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol (⚙).
   - Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile** → 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 Programmen von Kaspersky 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.

So konfigurieren Sie den Export in SIEM-Systeme in Kaspersky Security Center Web Console:

1. Klicken Sie im Hauptmenü neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   Das Eigenschaftenfenster des Administrationsservers wird geöffnet.

2. Wählen Sie auf der Registerkarte **Allgemein** den Abschnitt **SIEM** 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 entweder die Protokolle TCP/IP, UDP oder TLS over TCP 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.

- **Name/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 **Name/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 PEM**. 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 PKCS12**. 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.

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. Setzen Sie die Option auf die Position **Auto-Exportieren von Ereignissen in die Datenbank des SIEM-Systems Aktiviert**.

7. Um zu überprüfen, ob die Verbindung mit dem SIEM-System erfolgreich konfiguriert wurde, klicken Sie auf die Schaltfläche **Verbindung prüfen**.

   Der Verbindungsstatus wird angezeigt.

8. Klicken Sie auf die Schaltfläche **Speichern**.

Der Export in ein SIEM-System ist konfiguriert. Wenn Sie das Empfangen von Ereignissen in einem SIEM-System konfiguriert haben, exportiert der Administrationsserver von nun an die markierten Ereignisse in ein SIEM-System. Wenn Sie das Startdatum des Exports angegeben haben, exportiert der Administrationsserver auch die markierten Ereignisse, die in der Datenbank des Administrationsservers ab dem angegebenen Datum gespeichert sind.

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, Programme oder Benutzer. Sie können diese Informationen beim Erstellen von Abfragen verwenden.

In diesem Abschnitt finden Sie Anweisungen zum Erstellen einer SQL-Abfrage mithilfe des Tools klsql2 sowie ein Beispiel einer solchen Anfrage.

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.

Erstellen einer SQL-Abfrage mithilfe des Tools klsql2

Dieser Artikel enthält die Beschreibung zur Verwendung des Tools "klsql2" sowie zum Erstellen 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 auf dem Gerät, auf dem der Kaspersky Security Center Administrationsserver installiert ist, in das Verzeichnis "/opt/kaspersky/ksc64/sbin/klsql2".

2. Erstellen Sie in diesem Verzeichnis eine leere Datei namens "src.sql".

3. Öffnen Sie die Datei src.sql in einem beliebigen Texteditor.

4. Geben Sie in die src.sql-Datei den von Ihnen gewünschten SQL-Query ein und speichern Sie die Datei.

5. Geben Sie auf dem Computer, auf dem der Kaspersky Security Center Administrationsserver installiert ist, in der Befehlszeile den folgenden Befehl für den Start der SQL-Abfrage aus der Datei src.sql 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 erstellte Datei result.xml und sehen Sie sich die Ergebnisse der Abfragenausführung an.

Sie können die Datei src.sql editieren und darin beliebige Anfragen der öffentlichen 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

In diesem Abschnitt ist als Beispiel eine SQL-Anfrage angeführt, die mithilfe des Tools klsql2 erstellt wurde.

Das folgende Beispiel zeigt, wie Sie eine Ereignisliste für die Ereignisse der letzten sieben Tage auf den Geräten der Benutzer erhalten und diese nach der Uhrzeit sortieren, zu der das Ereignis aufgetreten ist, wobei die aktuellsten Ereignisse zuerst angezeigt werden.

Beispiel:
```
SELECT
```

```
e. nId, /* ID des Ereignisses */
e. tmRiseTime, /* Uhrzeit, zu der das Ereignis aufgetreten ist */
e. strEventType, /* interner Name des Ereignistyps */
e. wstrEventTypeDisplayName, /* angezeigter Name des Ereignisses */
e. wstrDescription, /* angezeigte Beschreibung des Ereignisses */
e. wstrGroupName, /* Name der Gerätegruppe */
h.wstrDisplayName, /* angezeigter Gerätename des Geräts, auf dem das Ereignis
aufgetreten ist */
CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* IP-Adresse des Geräts, auf dem das
Ereignis aufgetreten ist */
FROM v_akpub_ev_event e
INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
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 neben dem Namen des benötigten Administrationsservers auf das Einstellungen-Symbol ( ).

   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.

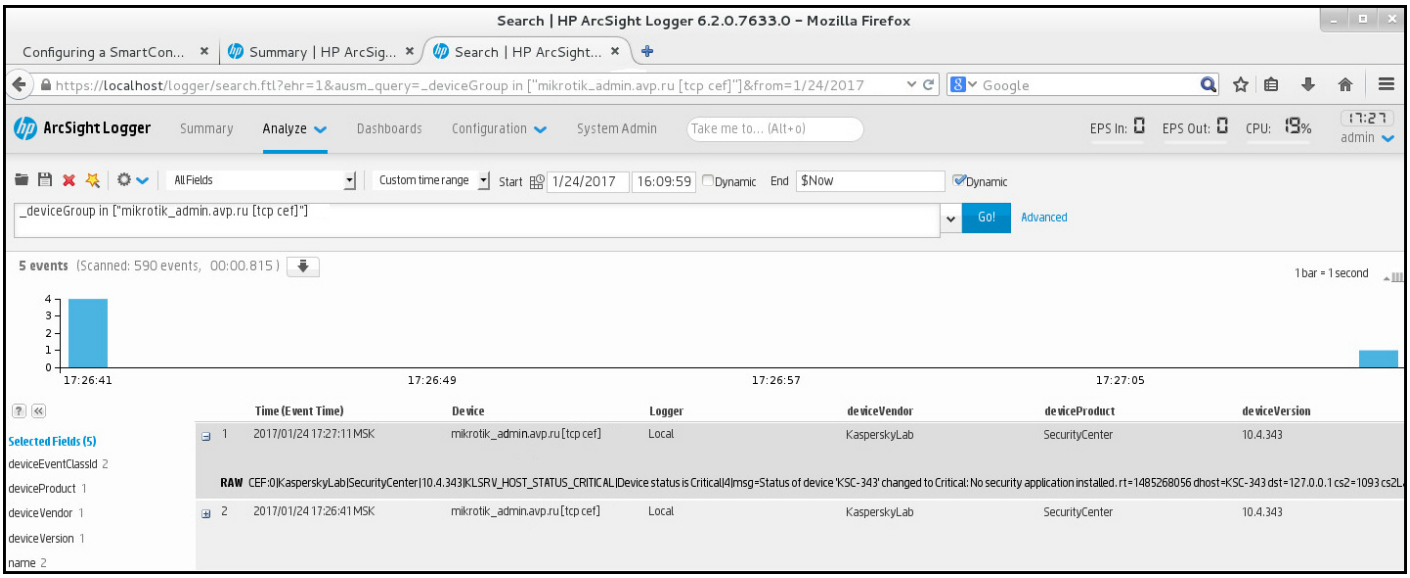
Exportergebnisse anzeigen

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.

Das Anzeigen und Speichern einer Richtlinienrevision ist verfügbar, wenn diese Funktionalität auch durch das entsprechende Web-Plug-in zur Verwaltung unterstützt wird.

So zeigen Sie eine Richtlinienrevision an:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Richtlinien und Profile**.
2. Klicken Sie auf die Richtlinie, deren Revision Sie anzeigen möchten, und wechseln Sie anschließend zum Abschnitt **Revisionsverlauf**.
3. Klicken Sie in der Liste mit den Richtlinienrevisionen auf die Nummer der Revision, die Sie anzeigen möchten.

   Wenn die Größe der Revision 10 MB überschreitet, 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 Größe der Revision 10 MB nicht überschreitet, werden die Einstellungen der ausgewählten Richtlinienrevision als Bericht im HTML-Format angezeigt. Da der Bericht in einem Pop-up-Fenster angezeigt wird, stellen Sie sicher, dass das Anzeigen von Pop-ups in Ihrem Browser erlaubt ist.

So speichern Sie eine Revision als JSON-Datei:

Wählen Sie in der Liste der Richtlinienrevisionen die Revision aus, die Sie speichern möchten, und klicken Sie anschließend auf **In Datei speichern**.

Die Revision wird in einer JSON-Datei gespeichert.

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.

Objekte löschen

Dieser Abschnitt bietet Informationen über das Löschen von Objekten und Anzeigen von Informationen über Objekte, nachdem sie gelöscht wurden.

Sie können Objekte löschen, einschließlich der folgenden:

- Richtlinien
- Aufgaben
- Installationspakete
- Virtuelle Administrationsserver
- Benutzer
- Sicherheitsgruppen
- Administrationsgruppen

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 **zum Ändern** im Berechtigungsbereich **Gelöschte Objekte** verfügen.

Über das Löschen von Client-Geräten

Wenn Sie ein verwaltetes Gerät aus einer Administrationsgruppe löschen, verschiebt das Programm 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. Um das Laufwerk zu entschlüsseln, müssen in diesem Fall 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 manuell aus der Gruppe "Nicht zugeordnete Geräte" löschen, entfernt das Programm das Gerät aus der Liste. Nach dem Löschen des Geräts verbleiben etwaige installierte Kaspersky -Programme 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 Backup herunterladen und löschen

Dieser Abschnitt enthält Informationen zum Herunterladen und Löschen von Dateien aus Quarantäne und Backup in der Kaspersky Security Center Web Console.

Dateien aus Quarantäne und Backup herunterladen

Sie können Dateien aus Quarantäne und Backup 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.

Um eine Kopie der Datei aus der Quarantäne oder dem Backup auf eine Festplatte zu speichern, gehen Sie wie folgt vor:

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 → Backup**.

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 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**, **Backup**, oder **Aktive Bedrohungen** von Kaspersky Security Center Linux. Wenn Sie einen dieser Abschnitte öffnen, ein Objekt aus der Liste auswählen und auf die Schaltfläche **Entfernen** klicken, führt Kaspersky Security Center Linux eine der folgenden Aktionen oder beide Aktionen aus:

- Es entfernt das ausgewählte Objekt aus der Liste

- Es löscht das ausgewählte Objekt aus der Datenverwaltung

Die auszuführende Aktion wird durch das Kaspersky-Programm festgelegt, welches das ausgewählte Objekt in der Datenverwaltung abgelegt hat. Das Kaspersky-Programm ist im Feld **Eintrag hinzugefügt von** angegeben. Für weitere Informationen, welche Aktion ausgeführt wird, wenden Sie sich bitte an die Dokumentation des jeweiligen Kaspersky-Programms.

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, gehen Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte**.
   - Wenn das Gerät zur Gruppe nicht zugeordneter Geräte gehört, wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung** → **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 im folgenden Fenster 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 **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme 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.

   - **Rotationsbasierte Ablaufverfolgung**

     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 **Programme von Kaspersky** 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 "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 **Xperf-Ablaufverfolgungsstufe ändern** eine der folgenden Ablaufverfolgungsstufen entsprechend den Anweisungen des Spezialisten des technischen Supports aus:

   a. Wählen Sie eine der folgenden Ablaufverfolgungsstufen aus:

   - **Oberflächlich**

     Eine Protokolldatei dieses Typs enthält die Mindestmenge an Informationen über das System.

     Diese Variante ist standardmäßig ausgewählt.

   - **Tief**

     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:

   - **Basistyp**

Die Ablaufverfolgungsinformationen werden während der Ausführung der Sicherheitsanwendung Kaspersky Endpoint Security empfangen.

Diese Variante ist standardmäßig ausgewählt.

- **Bei-Neustart-Typ**

  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 **Programme von Kaspersky** 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 **Dateiende herunterladen**.

Das gleichzeitige Herunterladen von Teilen mehrerer Dateien ist nicht möglich. Wenn Sie mehr als eine Protokolldatei auswählen, wird die Schaltfläche **Dateiende 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-Installationen**, 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 **Programme von Kaspersky** aus.
3. Klicken Sie im Abschnitt **Programmeinstellungen** 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.

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 durch klicken auf **Vollständige Datei herunterladen** herunter.
   - Um einen Teil des ausgewählten Protokolls herunterzuladen:

     a. Klicken Sie auf die Schaltfläche **Dateiende herunterladen**.

     Das gleichzeitige Herunterladen von Teilen mehrerer Protokolle ist nicht möglich. Wenn Sie mehr als ein Ereignisprotokoll auswählen, wird die Schaltfläche **Dateiende 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 **Programme von Kaspersky** 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:

   - **Programm beenden**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.
   - **Programm neu starten**

     Diese Schaltfläche ist nur verfügbar, wenn das Programm gerade ausgeführt wird.
   - **Programm 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 **Programme von Kaspersky** aus.

   Im Abschnitt **Programmverwaltung** wird die Liste der auf dem Gerät installierten Kaspersky-Programme 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 Supportspezialist von Kaspersky Sie dazu auffordert. Sie müssen das Programm nicht auf dem Gerät installieren.

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. Klicken Sie im Abschnitt **Programmdateien** auf die Schaltfläche **Durchsuchen**, um ein zip-Archiv auszuwählen, das die Anwendung enthält, die Sie auf dem Client-Gerät ausführen möchten.

   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.

   Bei Bedarf können Sie den Namen der ausführbaren Datei und die Befehlszeilenargumente angeben. Füllen Sie dazu die Felder **Archivierte ausführbare Datei, die auf einem Remote-Gerät ausgeführt werden soll** und **Befehlszeilenargumente** aus.
4. Klicken Sie auf die Schaltfläche **Hochladen und ausführen**, um die angegebene Anwendung auf einem Client-Gerät auszuführen.
5. Folgen Sie den Anweisungen des Experten vom Kaspersky-Support.

Erzeugen einer Dump-Datei für eine Anwendung

Mit einer Dump-Datei für eine Anwendung können Sie die Parameter der Anwendung anzeigen, die an einem bestimmten Zeitpunkt auf einem Client-Gerät ausgeführt wird. Diese Datei enthält auch Informationen über die Module, die für eine Anwendung geladen wurden.

Das Generieren von Dump-Dateien ist nur für 32-Bit-Prozesse verfügbar, die auf Windows-basierten Client-Geräten ausgeführt werden. Diese Funktion wird für Linux-Client-Geräte und 64-Bit-Prozesse nicht unterstützt.

So erzeugen Sie eine Dump-Datei für eine Anwendung:

1. Öffnen Sie auf einem Client-Gerät das Fenster für die Ferndiagnose.
2. Wählen Sie im Ferndiagnose-Fenster die Registerkarte **Remote-Ausführung einer Anwendung** aus.
3. Geben Sie im Abschnitt **Dump-Datei für den Prozess erstellen** die ausführbare Datei der Anwendung an, für die Sie eine Dump-Datei erstellen möchten.
4. Klicken Sie auf die Schaltfläche **Herunterladen**, um die Dump-Datei für die angegebene Anwendung zu speichern.

   Wenn die angegebene Anwendung nicht auf dem Client-Gerät ausgeführt wird, erscheint eine Fehlermeldung.

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-Programme auf Client-Geräten verwalten

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center Linux für die Verwaltung von Drittanbieter-Programmen beschrieben, die auf Client-Geräten ausgeführt werden.

Über Anwendungen von Drittanbietern

Kaspersky Security Center Linux kann Ihnen dabei helfen, auf Client-Geräten installierte Software von Drittanbietern zu aktualisieren und die Schwachstellen in der Software von Drittanbietern zu beheben. Kaspersky Security Center Linux kann Software von Drittanbietern nur von der aktuell installierten Version auf die neueste Version aktualisieren. Die folgende Liste stellt die Software von Drittanbietern dar, die Sie mit Kaspersky Security Center Linux aktualisieren können:

Die Liste der Software von Drittanbietern kann aktualisiert und um neue Anwendungen erweitert werden. Sie können überprüfen, ob Sie die Software von Drittanbietern (die auf den Geräten der Benutzer installiert ist) mit Kaspersky Security Center Linux aktualisieren können, indem Sie die Liste der verfügbaren Updates in der Kaspersky Security Center Web Console anzeigen.

- 7-Zip-Developers: 7-Zip
- Adobe-Systems:
  - Adobe Acrobat DC
  - Adobe Acrobat Reader DC
  - Adobe Acrobat
  - Adobe Reader
  - Adobe Shockwave Player
- AIMPDevTeam: AIMP
- ALTAP: Altap Salamander
- Apache Software Foundation: Apache Tomcat
- Apple:
  - Apple iTunes
  - Apple QuickTime
- Armory Technologies, Inc.: Armory
- Cerulean Studios: Trillian Basic
- Ciphrex Corporation: mSIGNA
- Cisco: Cisco Jabber

- Code Sector: TeraCopy
- Codec Guide:
  - K-Lite Codec Pack Basic
  - K-Lite Codec Pack Full
  - K-Lite Codec Pack Mega
  - K-Lite Codec Pack Standard
- DbVis Software AB: DbVisualizer
- Decho Corp.:
  - Mozy Enterprise
  - Mozy Home
  - Mozy Pro
- Dominik Reichl: KeePass Password Safe
- Don HO don.h@free.fr: Notepad++
- DoubleGIS: 2GIS
- Dropbox, Inc.: Dropbox
- EaseUs: EaseUS Todo Backup Free
- Electrum Technologies GmbH: Electrum
- Enter Srl: Iperius Backup
- Eric Lawrence: Fiddler
- EverNote: EverNote
- Exodus Movement Inc: Exodus
- EZB Systems: UltraISO
- Famatech:
  - Radmin
  - Remote Administrator
- Far Manager: FAR Manager
- FastStone Soft: FastStone Image Viewer
- FileZilla Project: FileZilla

- Firebird Developers: Firebird
- Foxit Corporation:
  - Foxit Reader
  - Foxit Reader Enterprise
- Free Download Manager.ORG: Free Download Manager
- GIMP-Projekt: GIMP
- GlavSoft LLC.: TightVNC
- GNU-Projekt: Gpg4win
- Google:
  - Google Earth
  - Google Chrome
  - Google Chrome Enterprise
  - Google Earth Pro
- Inkscape-Projekt: Inkscape
- IrfanView: IrfanView
- iterate GmbH: Cyberduck
- Logitech: SetPoint
- LogMeIn, Inc.:
  - LogMeIn
  - Hamachi
  - LogMeIn Rescue Technician Console
- Martin Prikryl: WinSCP
- Microsoft: SQL Server Management Studio
- Mozilla Foundation:
  - Mozilla Firefox
  - Mozilla Firefox ESR
  - Mozilla SeaMonkey
  - Mozilla Thunderbird

- New Cloud Technologies Ltd: MyOffice Standard. Home Edition
- OpenOffice.org: OpenOffice
- Opera Software: Opera
- Oracle Corporation:
  - Oracle Java JRE
  - Oracle VirtualBox
- PDF44: PDF24 MSI/EXE
- Piriform:
  - CCleaner
  - Defraggler
  - Recuva
  - Speccy
- Postgresql: PostgreSQL
- RealNetworks: RealPlayer Cloud
- RealVNC:
  - RealVNC Server
  - RealVNC Viewer
- Right Hemisphere Inc.: SAP Visual Enterprise Viewer (Complete/Minimum)
- Simon Tatham: PuTTY
- Skype Technologies: Skype for Windows
- Sober Lemur S.a.s.:
  - PDFsam Basic
  - PDFsam Visual
- Softland: FBackup
- Splashtop Inc.: Splashtop Streamer
- Stefan Haglund, Fredrik Haglund, Florian Schmitz: CDBurnerXP
- Sublime HQ Pty Ltd: Sublime Text
- TeamViewer GmbH:

    - TeamViewer Host
    - TeamViewer
- Telegram Messenger LLP: Telegram Desktop
- The Document Foundation:
    - LibreOffice
    - LibreOffice HelpPack
- The Git Development Community:
    - Git for Windows
    - Git LFS
- The Pidgin developer community: Pidgin
- TortoiseSVN Developers: TortoiseSVN
- VideoLAN: VLC media player
- VMware:
    - VMware Player
    - VMware Workstation
- WinRAR Developers: WinRAR
- WinZip: WinZip
- Wireshark Foundation: Wireshark
- Wrike: Wrike
- Zimbra: Zimbra Desktop

Szenario: Programmverwaltung

Sie können den Start von Programmen auf Benutzergeräten verwalten. Sie können zulassen oder blockieren, dass Programme auf verwalteten Geräten ausgeführt werden. Verwenden Sie dazu die Komponente "Programmkontrolle". Sie können nur Programme verwalten, die auf Windows- oder Linux-Geräten installiert sind.

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.

Schritte

Die Nutzung der Programmkontrolle erfolgt schrittweise:

1. **Erstellen und Anzeigen der Liste der Programme auf Client-Geräten**

   Dieser Schritt unterstützt Sie dabei, herauszufinden, welche Programme auf den verwalteten Geräten installiert sind. Sie können die Liste der Programme anzeigen und gemäß den Sicherheitsrichtlinien Ihres Unternehmens entscheiden, welche Programme zulässig oder verboten sein sollen. Die Einschränkungen können sich auf die Informationssicherheitsrichtlinien des Unternehmens beziehen. Sie können diese Phase überspringen, wenn Sie genau wissen, welche Programme auf den verwalteten Geräten installiert sind.

   Anleitung: Liste der auf Client-Geräten installierten Anwendungen abrufen und anzeigen

2. **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. Sie können diesen Schritt überspringen, wenn Sie genau wissen, welche ausführbaren Dateien auf verwalteten Geräten installiert sind.

   Anleitungen: Liste der auf Client-Geräten gespeicherten ausführbaren Dateien abrufen und anzeigen

3. **Erstellen von Programmkategorien für die im Unternehmen verwendeten Programme**

   Analysieren Sie die Listen der Programme und ausführbaren Dateien, die auf verwalteten Geräten gespeichert sind. Erstellen Sie Programmkategorien anhand der Analyse. Es wird empfohlen, die Kategorie "Arbeitsprogramme" zu erstellen, welche die Standardprogramme enthält, die im Unternehmen verwendet werden. Wenn verschiedene Sicherheitsgruppen unterschiedliche Programmgruppen verwenden, können Sie für jede Sicherheitsgruppe eine separate Programmkategorie erstellen.

   Abhängig von den Kriterien zum Erstellen einer Programmkategorie können Sie zwei Typen von Programmkategorien erstellen.

   Anleitung: Manuell zu erweiternde Programmkategorie erstellen, Programmkategorie mit ausführbaren Dateien aus ausgewählten Geräten erstellen

4. **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 Programmkategorien, die Sie beim vorherigen Schritt erstellt haben.

   Anleitung: Konfigurieren der Programmkontrolle in der Richtlinie von Kaspersky Endpoint Security für Windows

5. **Aktivieren der Komponente "Programmkontrolle" im Testbetrieb**

   Um sicherzustellen, dass die Regeln der Programmkontrolle nicht die für die Benutzerarbeit erforderlichen Programme 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 Anwendungen, 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**.

6. **Ändern der Einstellungen für Programmkategorien der Komponente "Programmkontrolle"**

   Nehmen Sie bei Bedarf Änderungen an den Einstellungen für die Programmkontrolle vor. Auf der Grundlage der Testergebnisse können Sie einer zu erweiternden Programmkategorie manuell ausführbare Dateien hinzufügen, die sich auf Ereignisse der Programmkontrolle beziehen.

   Anleitung für Kaspersky Security Center Web Console: Ereignisbezogene ausführbare Dateien zur Programmkategorie hinzufügen

7. **Anwenden der Regeln der Programmkontrolle im Funktionsmodus**

   Nachdem die Regeln der "Programmkontrolle" getestet wurden und die Konfiguration der Programmkategorien komplett 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**.

8. **Überprüfen der Konfiguration der Programmkontrolle**

   Stellen Sie sicher, dass folgende Aktionen ausgeführt wurden:

   - Erstellen von Programmkategorien
   - Konfigurieren der Programmkontrolle mit den Programmkategorien
   - Anwenden der Regeln der Programmkontrolle im Funktionsmodus

Ergebnisse

Wenn das Szenario abgeschlossen ist, wird der Start von Programmen auf verwalteten Geräten gesteuert. Die Benutzer können nur jene Programme starten, die in Ihrem Unternehmen erlaubt sind. Im Unternehmen verbotene Programme 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.

Über die Programmkontrolle

Die Komponente "Programmkontrolle" überwacht die Versuche von Benutzern, Programme zu starten, und reguliert mithilfe der Regeln der "Programmkontrolle" den Start von Programmen.

Die Komponente "Programmkontrolle" ist für Kaspersky Endpoint Security 11.2 für Linux und neuere Versionen verfügbar.

Das Starten von Programmen, 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 Programme mit Ausnahme der in den Regeln zum Blockieren angegebenen Programme zulassen möchten. Dieser Modus ist standardmäßig festgelegt.

- *Allow-Liste*. Dieser Modus wird verwendet, wenn Sie den Start aller Programme mit Ausnahme der in den Regeln zum Zulassen angegebenen Programme blockieren möchten.

Die Regeln der Programmkontrolle sind durch Programmkategorien implementiert. Sie erstellen Programmkategorien, die bestimmte Kriterien definieren. In Kaspersky Security Center Linux gibt es drei Arten von Programmkategorien:

- 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.

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 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 Programme und leitet die Liste an den Administrationsserver weiter. Es dauert etwa 10-15 Minuten, bis der Administrationsagent die Programmliste aktualisiert hat.

Bei Windows-basierten Client-Geräten erhält der Administrationsagent die meisten Informationen über installierte Programme aus der Windows-Registrierung. Bei Linux-basierten Client-Geräten werden dem Administrationsagenten die Informationen über installierte Programme durch die Paketmanager bereitgestellt.

Um die Liste mit auf verwalteten Geräten installierten Programmen anzusehen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.

   Die Seite zeigt eine Tabelle mit den Programmen an, die auf verwalteten Geräten installiert sind. Wählen Sie ein Programm aus, um seine Eigenschaften anzeigen, z. B. Name des Anbieters, Versionsnummer, Liste der ausführbaren Dateien, Liste der Geräte mit dem installierten Programm.

2. Sie können die Daten der Tabelle mit installierten Programmen wie folgt gruppieren und filtern:

   - Klicken Sie auf das Einstellungssymbol ( ) in der oberen rechten Ecke der Tabelle.

     Wählen Sie im geöffneten Menü **Columns settings** die Spalten aus, die in der Tabelle angezeigt werden sollen. Um den Betriebssystemtyp der Client-Geräte anzuzeigen, auf denen das Programm installiert ist, wählen Sie die Spalte **Typ des Betriebssystems** aus.

   - Klicken Sie auf das Filtersymbol ( ) 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 Programme wird angezeigt.

So zeigen Sie eine Liste der Programme an, die auf bestimmten verwalteten Geräten installiert sind:

Wechseln Sie im Hauptmenü zu **Geräte** → **Verwaltete Geräte** → **<Gerätename>** → **Erweitert** → **Programm-Registry**. In diesem Menü können Sie die Liste der Programme 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 Security für Windows.

Liste der auf Client-Geräten gespeicherten ausführbaren Dateien abrufen und anzeigen

Sie können eine Liste der auf verwalteten Geräten gespeicherten ausführbaren Dateien abrufen. Um ausführbare Dateien zu inventarisieren, müssen Sie eine Inventarisierungsaufgabe erstellen.

Für Kaspersky Endpoint Security für Linux ist die Funktion zur Inventarisierung ausführbarer Dateien erst seit Version 11.2 verfügbar.

Um eine Inventarisierungsaufgabe für ausführbare Dateien auf den Client-Geräten zu erstellen, gehen Sie folgendermaßen vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **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 **Programm** 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.

Während der Inventarisierung werden ausführbare Dateien folgender Formate erkannt: mz, com, pe, ne, sys, cmd, bat, ps1, js, vbs, reg, msi, cpl, dll, jar, sowie HTML-Dateien.

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 **Vorgänge** → **Drittanbieter-Programme** → **Ausführbare Dateien**.

Auf der Seite wird die Liste der auf Client-Geräten gespeicherten ausführbaren Dateien angezeigt.

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 **Vorgänge** → **Drittanbieter-Programme** → **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. Wählen Sie im Schritt **Bedingungskriterien** einen Regeltyp zum Erstellen einer Kategorie aus der Liste aus:

   - **Aus der KL-Kategorie**

     Wenn Sie diese Variante wählen, können Sie als Bedingung für die Aufnahme von Programmen in eine benutzerdefinierte Kategorie die Programmkategorie von Kaspersky angeben. Programme, die zur angegebenen Kaspersky-Kategorie gehören, werden in die benutzerdefinierte Programmkategorie aufgenommen.

   - **Zertifikat aus Datenverwaltung auswählen**

     Wenn Sie diese Variante wählen, können Sie Zertifikate aus der Datenverwaltung für Zertifikate angeben. Ausführbare Dateien, die gemäß dem angegebenen Zertifikat signiert sind, werden zur Benutzerkategorie hinzugefügt.

   - **Pfad des Programms 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 das Programm ausgeführt wird. Die auf dem ausgewählten Datenträgertyp ausgeführten Programme werden in die benutzerdefinierte Programmkategorie aufgenommen.

- **Hash, Metadaten oder Zertifikat**:
  - Aus Liste der ausführbaren Dateien auswählen

    Wenn Sie diese Variante wählen, können Sie die Programme, 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. Sie können ein Programm aus der Registry auswählen und die folgenden Dateimetadaten angeben:

    - Dateiname.
    - Dateiversion. Sie können den genauen Wert der Version angeben oder eine Bedingung beschreiben, z. B. "größer als 5.0".
    - Programmname.
    - Programmversion. Sie können den genauen Wert der Version angeben oder eine Bedingung beschreiben, z. B. "größer als 5.0".
    - Hersteller.

  - Manuell angeben

Wenn Sie diese Option wählen, müssen Sie als Bedingung für die Aufnahme von Programmen in eine benutzerdefinierte Kategorie Datei-Hash, Metadaten oder Zertifikat angeben.

Dateihash

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 berechneten Hash-Funktionen werden in der Datenbank des Administrationsservers gespeichert. Das Speichern der Hash-Funktionen vergrößert geringfügig den Umfang der Datenbank.

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 unterstützen 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 alle in Ihrem Netzwerk installierten Instanzen von Sicherheits-Apps das Programm Kaspersky Endpoint Security für Linux darstellen, 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 Metadaten werden an den Administrationsserver weitergegeben. Ausführbare Dateien mit denselben Metadaten werden in die Programmkategorie aufgenommen.

Zertifikat

Wenn Sie diese Variante wählen, können Sie Zertifikate aus der Datenverwaltung für Zertifikate angeben. Ausführbare Dateien, die gemäß dem angegebenen Zertifikat signiert sind, werden zur Benutzerkategorie hinzugefügt.

- 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 Programme 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:

- **Dateihash**

  Sie wählen aus, mit welcher Hash-Funktion (MD5 oder SHA256) die Hash-Werte berechnet werden sollen. Programme, die denselben Hash-Wert haben wie die Dateien in dem archivierten Ordner, werden in die benutzerdefinierte Programmkategorie aufgenommen.

  Wählen Sie nur dann eine MD5-Hash-Funktion aus, 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.

Wenn diese Option ausgewählt ist, können Sie eine Datei eines archivierten Ordners angeben und dann auswählen, welche Bedingung Sie verwenden möchten, um Programme 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:

- **Dateihash**

  Sie wählen aus, mit welcher Hash-Funktion (MD5 oder SHA256) die Hash-Werte berechnet werden sollen. Programme, die denselben Hash-Wert haben wie die Dateien in dem archivierten Ordner, werden in die benutzerdefinierte Programmkategorie aufgenommen.

  Wählen Sie nur dann eine MD5-Hash-Funktion aus, 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.

Das ausgewählte Kriterium wird zur Liste mit Kriterien hinzugefügt.

Sie können so viele Kriterien in die erstellende Programmkategorie aufnehmen, wie Sie benötigen.

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.

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. Sie wird 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.

Um eine Programmkategorie zu erstellen, die ausführbare Dateien von ausgewählten Geräten enthält, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **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. Folgen Sie den Anweisungen des Assistenten mithilfe der Schaltfläche **Weiter**.

3. Geben Sie in dem Schritt **Methode zum Erstellen der Kategorie auswählen** den Kategorienamen ein und wählen Sie die **Kategorie für ausführbare Dateien von ausgewählten Geräten. Diese ausführbaren Dateien werden automatisch verarbeitet und deren Metriken werden zur Kategorie hinzugefügt** 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 berechneten Hash-Funktionen werden in der Datenbank des Administrationsservers gespeichert. Das Speichern der Hash-Funktionen vergrößert geringfügig den Umfang der Datenbank.

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 unterstützen 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 alle in Ihrem Netzwerk installierten Instanzen von Sicherheits-Apps das Programm Kaspersky Endpoint Security für Linux darstellen, 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 Programmkategorie erstellt. Sie wird in der Liste der Programmkategorien angezeigt. Sie können die erstellte Programmkategorie verwenden, wenn Sie die "Programmkontrolle" anpassen.

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 Programmkategorie zu erstellen, die ausführbare Dateien aus dem ausgewählten Ordner enthält:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **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. 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 Programmen, 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 Programmkategorie 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 die Dateien der Kategorie berechnen (unterstützt von Kaspersky Endpoint Security 10 Service Pack 2 für Windows und höher) / MD5 für die Dateien der Kategorie berechnen (unterstützt von Vorgängerversionen von 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 berechneten Hash-Funktionen werden in der Datenbank des Administrationsservers gespeichert. Das Speichern der Hash-Funktionen vergrößert geringfügig den Umfang der Datenbank.

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 unterstützen 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 alle in Ihrem Netzwerk installierten Instanzen von Sicherheits-Apps das Programm Kaspersky Endpoint Security für Linux darstellen, 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 Programmkategorie erstellt. Sie wird in der Liste der Programmkategorien angezeigt. Sie können die Programmkategorie 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 angepassten Programmkategorien und die Einstellungen der einzelnen Programmkategorien anzeigen.

Um die Liste der Programmkategorien anzuzeigen,

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programmkategorien**.

Die Seite mit einer Liste der Programmkategorien wird angezeigt.

Um die Eigenschaften einer Programmkategorie anzuzeigen,

Klicken Sie auf den Namen der Programmkategorie.

Das Eigenschaftenfenster der Programmkategorie wird angezeigt. Die Eigenschaften sind auf mehreren Registerkarten angeordnet.

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 **Assets (Geräte)** → **Richtlinien und Profile**.

   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 **Programmeinstellungen** → **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 Programmen 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 Programmen 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 Programmen 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 den Computer nach Auswahl der Option **Laden von DDL-Modulen überwachen** neu, wenn Kaspersky Endpoint Security für Windows alle DLL-Module und -Treiber überwachen soll, einschließlich jener, 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 Programmstarts 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.

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:

- **Programmstart verboten** (*kritisches* Ereignis). Dieses Ereignis wird angezeigt, wenn Sie die Programmkontrolle so konfiguriert haben, dass Regeln angewendet werden.
- **Der Start des Programms 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 Programmstarts** (Ereignistyp *Warnung*). Dieses Ereignis wird angezeigt, wenn Sie in der "Programmkontrolle" das Anwenden von Regeln festgelegt haben, und ein Benutzer

auf ein Programm 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 und Berichterstattung → 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 zum Ereignis gehörenden ausführbaren Datei** 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:

  - **Zertifikatdaten (oder SHA256-Hashs für Dateien ohne ein Zertifikat)**

    Die Dateien können vom Zertifikat signiert werden. Dabei können von einem Zertifikat mehrere Dateien signiert werden. Beispielsweise können verschiedene Versionen eines Programms von einem Zertifikat signiert sein oder mehrere verschiedene Programme 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.

    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 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.

  - **Zertifikatdaten (Dateien ohne ein Zertifikat werden übersprungen)**

    Die Dateien können vom Zertifikat signiert werden. Dabei können von einem Zertifikat mehrere Dateien signiert werden. Beispielsweise können verschiedene Versionen eines Programms von einem Zertifikat signiert sein oder mehrere verschiedene Programme 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 die Version 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 Programmversion.

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.

Installieren von Software-Updates von Drittanbietern

In diesem Abschnitt werden die Funktionen von Kaspersky Security Center Linux für die Installation von Updates für Programme von Drittanbietern beschrieben, die auf Client-Geräten installiert sind.

Über Software-Updates von Drittanbietern

Mit Kaspersky Security Center Linux können Sie Updates für Software von Drittanbietern, die auf den verwalteten Geräten installiert ist, verwalten und Schwachstellen in dieser Software durch die Installation der erforderlichen Updates 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 installierte Software von Drittanbietern, die Sie in den Eigenschaften der Aufgabe angegeben haben. Nach dem Prüfen der Informationen über die verfügbaren Updates können Sie die Installation von Updates auf Ihren Geräten durchführen.

Das Update einiger Programme von Kaspersky Security Center Linux wird mittels Deinstallation der vorherigen Programmversion und Installation der neuen Version durchgeführt.

Eine Benutzerinteraktion kann erforderlich sein, 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 Software-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 Prüfung von Dateien verwendet und umfassen die Untersuchung auf Viren, die statische und die dynamische Analyse, die Verhaltensanalyse in der Sandbox-Umgebung, sowie Machine Learning-Methoden.

Kaspersky-Experten führen keine manuelle Analyse von Software-Updates von Drittanbietern 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 im obigen Abschnitt genannten hinausgehen.

Wenn die Metadaten der Software-Updates von Drittanbietern in die Datenverwaltung heruntergeladen wurden, können Sie die Updates mithilfe 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 entsprechen, die in den Update-Regeln angegeben sind. 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-Software, die auf den Client-Geräten installiert ist. Als Drittanbieter-Software gelten Anwendungen von anderen Softwareherstellern.

Erforderliche Vorrausetzungen

Der Administrationsserver muss mit dem Internet verbunden sein, um Software-Updates von Drittanbietern installieren zu können.

Schritte

Das Aktualisieren von Software von Drittanbietern erfolgt in mehreren Phasen:

1. **Suchen nach erforderlichen Updates**

   Führen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* aus, um die für die verwalteten Geräte erforderlichen Software-Updates von Drittanbietern 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 installierte Software von Drittanbietern, die Sie in den Eigenschaften der Aufgabe 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 *Finden von Schwachstellen und erforderlichen Updates* suchen nur für Windows-Geräte erstellen. Sie können diese Aufgabe nicht für Geräte mit anderen Betriebssystemen erstellen.

2. **Liste der gefundenen Updates anzeigen**

   Zeigen Sie Informationen zu verfügbaren Software-Updates von Drittanbietern an und entscheiden Sie, welche Updates Sie installieren möchten. Um detaillierte Informationen über alle Updates anzuzeigen, klicken Sie in der Liste auf den Namen des Updates. Für jedes Update in der Liste können Sie auch die Statistiken zur Update-Installation auf Client-Geräten anzeigen.

3. **Konfigurieren der Installation von Updates**

   Wenn Kaspersky Security Center Linux die Liste der Software-Updates von Drittanbietern 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 Software-Updates installieren zu können, müssen Sie deren Endbenutzer-Lizenzverträge (EULA) akzeptieren. Wenn Sie die EULA ablehnen, wird das Software-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. **Planen der Aufgaben**

   Um sicherzustellen, dass die Liste der Updates immer auf dem neuesten Stand ist, planen Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* so, dass sie regelmäßig automatisch ausgeführt wird. Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird standardmäßig wird standardmäßig manuell gestartet.

   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. **Genehmigen und Ablehnen der Software-Updates von Drittanbietern (optional)**

   Falls Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* erstellt haben, können Sie in den 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 setzen Sie für jene Updates, die Sie installieren möchten, manuell den Status *Genehmigt*. In diesem Fall werden Updates, die den Status *Nicht definiert* oder *Abgelehnt* besitzen, auf den in der Aufgabe angegebenen Servern nicht installiert.

   Bei einer geringen Menge an Updates ist das Verwenden des Status *Genehmigt* für die Verwaltung der Installation der Updates ist effizient. Für die Verwaltung mehrerer Updates können Sie die Regeln verwenden, die Sie in der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* 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 große Anzahl von Updates manuell genehmigen, verringert sich die Leistung des Administrationsservers, was zu einer Überlastung des Administrationsservers führen kann.

   Standardmäßig besitzen heruntergeladene Software-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 der Vorgehensweise zum Genehmigen und Ablehnen von Software-Updates von Drittanbietern.

6. **Ausführen einer Aufgabe zum Installieren von Updates**

   Starten der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen*. Wenn Sie diese Aufgabe starten, werden die Updates heruntergeladen und auf den verwalteten Geräten installiert. Stellen Sie nach Abschluss der Aufgabe sicher, dass sie in der Liste den Status *Erfolgreich beendet* besitzt.

7. **Erstellen eines Bericht über die Ergebnisse der Update-Installation (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 wurden, 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 für Software-Updates von Drittanbietern

Sie können Software-Updates von Drittanbietern und Updates von 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 die Software anderer Hersteller installieren.

Eine Benutzerinteraktion kann erforderlich sein, 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.

  Als Ergebnis wird eine neue Aufgabe zum Installieren der ausgewählten Updates erstellt. Optional können Sie die ausgewählten Updates zu einer existierenden Aufgabe hinzufügen.

- Indem Sie den Assistenten zur Installation von Updates ausführen.

  Der Update-Installationsassistent ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

  Der Assistent vereinfacht die Erstellung und Konfiguration einer Aufgabe zum Konfigurieren der Update-Installation und ermöglicht es Ihnen, die Erstellung redundanter Aufgaben zu vermeiden, die dieselben zu installierenden Updates enthalten.

Installieren von Software-Updates von Drittanbietern mithilfe der Update-Liste

So installieren Sie Software-Updates von Drittanbietern mithilfe der Update-Liste:

1. Öffnen Sie die Update-Liste über einen der folgenden Wege:

   - **Vorgänge** → **Patch-Management** → **Software-Updates**.
   - **Assets (Geräte)** → **Verwaltete Geräte** → <Gerätename> → **Erweitert** → **Verfügbare Updates**.
   - **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry** → <Name des Programms> → **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 die Schaltfläche **Updates installieren**. Wenn diese Schaltfläche nicht sichtbar ist, klicken Sie auf die Schaltfläche mit den drei Punkten und wählen Sie anschießend in der Dropdown-Liste die Option **Updates installieren** aus.

   Zum Installieren bestimmter Software-Updates müssen Sie den Endbenutzer-Lizenzvertrag (EULA) akzeptieren. Wenn Sie die EULA ablehnen, wird das Software-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, wird 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 wollen. 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 gewählten Updates wurde der ausgewählten Aufgabe automatisch hinzugefügt. Die ausgewählten Updates wurden 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 in der Aufgabenliste unter **Assets (Geräte)** → **Aufgaben** angezeigt. Wenn Sie sich entschieden haben, die Aufgaben zu einer existierenden Aufgabe hinzuzufügen, werden die Updates in den Aufgabeneigenschaften gespeichert.

Um Software-Updates von Drittanbietern zu installieren, müssen Sie die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* starten. Sie können diese Aufgabe starten, indem Sie in der Aufgabenliste auf die Schaltfläche **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 Software-Updates von Drittanbietern mithilfe des Assistenten zur Installation von Updates

Der Update-Installationsassistent ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Um eine Aufgabe zur Installation der Software-Updates von Drittanbietern mithilfe des Assistenten zur Installation von Updates zu installieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **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 die Schaltfläche **Assistent zur Installation von Updates starten**.

   Der Assistent zur Installation von Updates wird gestartet. Die Seite **Wählen Sie die Aufgabe zur Installation von Updates aus** zeigt Ihnen die Liste aller existierenden 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 soll, aktivieren Sie die Option **Nur Aufgaben anzeigen, die das Update installieren**.

5. Wählen Sie, was Sie tun 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 die Schaltfläche **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 die Schaltfläche **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 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 von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Schweregrad des ausgewählten Updates (**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 nicht angezeigt, wenn die Ereigniskategorie des ausgewählten Updates *Unbekannt* ist.

     - 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 Software-Updates von Microsoft angezeigt. Sie wird nicht angezeigt, wenn die Ereigniskategorie des ausgewählten Updates *Unbekannt* ist.

- **Regel für die Installation von Updates dieses Herstellers**

  Diese Option ist nur für Updates von Dritthersteller-Anwendungen verfügbar. Kaspersky Security Center Linux installiert nur die Updates, die sich auf Programme beziehen, die vom selben Anbieter wie das ausgewählte Update erstellt wurden. Abgelehnte Updates und Updates für Programme anderer Anbieter werden nicht installiert.

  Diese Option ist standardmäßig deaktiviert.

  Diese Regel wird nur für Software-Updates von Drittanbietern angezeigt.

- **Regel für die Installation von Updates vom Typ**
- **Regel für die Installation von Updates des ausgewählten Programms**

  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 Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

Lassen Sie diese Option optimiert, wenn Sie mit der Installation von Programmzwischenversionen einverstanden sind, wenn 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 eine geradlinige Weist 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.

Wenn Sie beispielsweise Version 3 eines Programms auf einem Gerät installiert haben und Sie es auf Version 5 aktualisieren möchten, Version 5 dieses Programms aber nur über Version 4 installiert werden kann. 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 bereits 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 die Schaltfläche **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 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 von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Schweregrad des ausgewählten Updates (**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 nicht angezeigt, wenn die Ereigniskategorie des ausgewählten Updates *Unbekannt* ist.

  - 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 Software-Updates von Microsoft angezeigt. Sie wird nicht angezeigt, wenn die Ereigniskategorie des ausgewählten Updates *Unbekannt* ist.

- Regel für die Installation von Updates dieses Herstellers

  Diese Option ist nur für Updates von Dritthersteller-Anwendungen verfügbar. Kaspersky Security Center Linux installiert nur die Updates, die sich auf Programme beziehen, die vom selben Anbieter wie das ausgewählte Update erstellt wurden. Abgelehnte Updates und Updates für Programme anderer Anbieter werden nicht installiert.

  Diese Option ist standardmäßig deaktiviert.

  Diese Regel wird nur für Software-Updates von Drittanbietern angezeigt.

- **Regel für die Installation von Updates vom Typ**

- **Regel für die Installation von Updates des ausgewählten Programms**

  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 Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren

Lassen Sie diese Option optimiert, wenn Sie mit der Installation von Programmzwischenversionen einverstanden sind, wenn 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 eine geradlinige Weist 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.

Wenn Sie beispielsweise Version 3 eines Programms auf einem Gerät installiert haben und Sie es auf Version 5 aktualisieren möchten, Version 5 dieses Programms aber nur über Version 4 installiert werden kann. 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 Aufgabe fort. Die neue Regel, die Sie im Assistenten zur Installation von Updates hinzugefügt haben, wird im Assistenten für das Erstellen einer Aufgabe 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, erstellen Sie die Aufgabe manuell.

Zusätzlich zu den allgemeinen Aufgabeneinstellungen können Sie die folgenden Einstellungen vornehmen, wenn Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* erstellen oder wenn Sie später die Eigenschaften der erstellten Aufgabe anpassen:

- **Nach Schwachstellen und Updates suchen, die von Microsoft gelistet werden**

  Wenn Kaspersky Security Center Linux nach Schwachstellen und Updates sucht, verwendet das Programm die Informationen über geeignete Microsoft-Updates aus der Quelle für momentan verfügbare Microsoft-Updates.

  Es wird empfohlen, diese Funktion zu deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft-Updates und Updates für Drittanbieter-Apps haben.

  Diese Option ist standardmäßig aktiviert.

- **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:

- Kaspersky Security Center Linux Administrationsserver (siehe Einstellungen der Richtlinie des Administrationsagenten)
- 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 jene Informationen über geeignete Microsoft-Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden und im Geräte-Cache gespeichert sind.

Das Herstellen einer Verbindung zur Update-Quelle von Microsoft kann viele Ressourcen in Anspruch nehmen. 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 festlegen. Wenn Sie diese Option nicht deaktivieren möchten, können Sie den Aufgabenzeitplan so anpassen, dass die Aufgabenstarts innerhalb von 360 Minuten zufällig verzögert werden, um so die Serverüberladung zu reduzieren.

Diese Option ist standardmäßig aktiviert.

Der Modus für den Update-Download beruht auf einer Kombination der folgenden Optionen, mit denen die Einstellungen der Administrationsagenten-Richtlinie festgelegt werden:

- Um Updates abzurufen, stellt der Windows Update-Agent auf einem verwalteten Gerät nur dann eine Verbindung zum Update-Server her, wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert ist und die Option **Aktiv** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.
- Der Windows Update-Agent auf einem verwalteten Gerät verwendet jene Informationen über geeignete Microsoft-Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden und im Geräte-Cache gespeichert sind, sofern die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert ist und die Option **Offline** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist, oder wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** deaktiviert ist und die Option **Aktiv** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.
- Unabhängig vom Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert) fordert Kaspersky Security Center Linux keine Informationen über Updates an, wenn die Option **Deaktiviert** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.

- Nach Schwachstellen und Updates von Drittherstellern 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 Programmen im Dateisystem an** festgelegten Ordnern nach Schwachstellen und erforderlichen Updates für Produkte Dritter (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden). Die vollständige Liste von unterstützten Drittanbieter-Apps wird von Kaspersky verwaltet.

Wenn diese Option deaktiviert ist, sucht Kaspersky Security Center Linux nicht nach Schwachstellen und erforderlichen Updates für Drittanbieter-Programme. Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft Windows-Updates und Updates für Drittanbieter-Apps 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-Apps sucht, für die ein Schließen von Schwachstellen und eine Update-Installation erforderlich ist. Sie können Systemvariable verwenden.

  Legen Sie die Ordner fest, in denen Apps installiert sind. Standardmäßig enthält die Liste Systemordner, in denen die meisten Apps installiert sind.

- **Erweiterte Diagnose aktivieren**

  Wenn diese Funktion aktiviert ist, führt der Administrationsagent die Ablaufverfolgung auch dann durch, wenn die Ablaufverfolgung für den Administrationsagenten im Tool zur 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, beginnt der Administrationsagent sie wieder von vorn zu überschreiben. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

  Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool zur Remote-Diagnose für Kaspersky Security Center Linux durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

  Beim Erstellen einer Aufgabe, müssen Sie die erweiterte Diagnose nicht aktivieren. Sie möchten diese Funktion möglicherweise später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen empfangen möchten.

  Diese Option ist standardmäßig deaktiviert.

- **Maximale Größe der Dateien für die erweiterte Diagnose (MB)**

  Der Standardwert beträgt 100 MB und verfügbare Werte liegen zwischen 1 MB und 2048 MB. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, wenn die Informationen in den von Ihnen gesendeten Dateien für die erweiterte 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.

Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird standardmäßig wird standardmäßig manuell gestartet. Wenn die Dienstvorschriften des Unternehmens zu diesem Zeitpunkt das Deaktivieren der Geräte vorsehen, 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 des Geräts veranlassen kann. Es ist erforderlich, den optimalen Zeitplan der Aufgabe ausgehend von den im Unternehmen geltenden Dienstvorschriften zu konfigurieren.

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 **Assets (Geräte)** → **Aufgaben**.
2. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Der Assistent für das Erstellen einer Aufgabe wird gestartet. Setzen Sie den Assistenten mithilfe der Schaltfläche **Weiter** fort.
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 das Programm die Informationen über geeignete Microsoft-Updates aus der Quelle für momentan verfügbare Microsoft-Updates.

     Es wird empfohlen, diese Funktion zu deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft-Updates und Updates für Drittanbieter-Apps haben.

     Diese Option ist standardmäßig aktiviert.

- 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:

  - Kaspersky Security Center Linux Administrationsserver (siehe Einstellungen der Richtlinie des Administrationsagenten)
  - 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 jene Informationen über geeignete Microsoft-Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden und im Geräte-Cache gespeichert sind.

  Das Herstellen einer Verbindung zur Update-Quelle von Microsoft kann viele Ressourcen in Anspruch nehmen. 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 festlegen. Wenn Sie diese Option nicht deaktivieren möchten, können Sie den Aufgabenzeitplan so anpassen, dass die Aufgabenstarts innerhalb von 360 Minuten zufällig verzögert werden, um so die Serverüberladung zu reduzieren.

  Diese Option ist standardmäßig aktiviert.

  Der Modus für den Update-Download beruht auf einer Kombination der folgenden Optionen, mit denen die Einstellungen der Administrationsagenten-Richtlinie festgelegt werden:

  - Um Updates abzurufen, stellt der Windows Update-Agent auf einem verwalteten Gerät nur dann eine Verbindung zum Update-Server her, wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert ist und die Option **Aktiv** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.
  - Der Windows Update-Agent auf einem verwalteten Gerät verwendet jene Informationen über geeignete Microsoft-Windows-Updates, die zuvor von der Quelle der Microsoft-Updates empfangen wurden und im Geräte-Cache gespeichert sind, sofern die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** aktiviert ist und die Option **Offline** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist, oder wenn die Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** deaktiviert ist und die Option **Aktiv** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.
  - Unabhängig vom Status der Option **Mit dem Update-Server verbinden, um Daten zu aktualisieren** (aktiviert oder deaktiviert) fordert Kaspersky Security Center Linux keine Informationen über Updates an, wenn die Option **Deaktiviert** in der Einstellungsgruppe **Modus für die Suche nach Windows-Updates** ausgewählt ist.

- Nach Schwachstellen und Updates von Drittherstellern 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 Programmen im Dateisystem an** festgelegten Ordnern nach Schwachstellen und erforderlichen Updates für Produkte Dritter (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden). Die vollständige Liste von unterstützten Drittanbieter-Apps wird von Kaspersky verwaltet.

Wenn diese Option deaktiviert ist, sucht Kaspersky Security Center Linux nicht nach Schwachstellen und erforderlichen Updates für Drittanbieter-Programme. Sie möchten diese Option beispielsweise deaktivieren, wenn Sie verschiedene Aufgaben mit unterschiedlichen Einstellungen für Microsoft Windows-Updates und Updates für Drittanbieter-Apps haben.

Diese Option ist standardmäßig aktiviert.

Sie können diese Optionen nach der Erstellung der Aufgabe auf der Registerkarte **Programmeinstellungen** 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-Apps sucht, für die ein Schließen von Schwachstellen und eine Update-Installation erforderlich ist. Sie können Systemvariable verwenden.

Legen Sie die Ordner fest, in denen Apps installiert sind. Standardmäßig enthält die Liste Systemordner, in denen die meisten Apps installiert sind.

Sie können die angegebenen Pfade nach der Erstellung der Aufgabe auf der Registerkarte **Programmeinstellungen** im Eigenschaftenfenster der Aufgabe ändern.

8. Aktivieren Sie bei Bedarf die Erweiterte Diagnose aktivieren

Wenn diese Funktion aktiviert ist, führt der Administrationsagent die Ablaufverfolgung auch dann durch, wenn die Ablaufverfolgung für den Administrationsagenten im Tool zur 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, beginnt der Administrationsagent sie wieder von vorn zu überschreiben. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool zur Remote-Diagnose für Kaspersky Security Center Linux durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

Beim Erstellen einer Aufgabe, müssen Sie die erweiterte Diagnose nicht aktivieren. Sie möchten diese Funktion möglicherweise später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen empfangen möchten.

Diese Option ist standardmäßig deaktiviert.

Sie können diese Option nach der Erstellung der Aufgabe auf der Registerkarte **Programmeinstellungen** 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 verfügbare Werte liegen zwischen 1 MB und 2048 MB. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, wenn die Informationen in den von Ihnen gesendeten Dateien für die erweiterte 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 **Programmeinstellungen** 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 bei der Aufgabenerstellung festgelegten Einstellungen ändern.

    Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Liste mit Aufgaben 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.

Die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* wird standardmäßig wird standardmäßig manuell gestartet.

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 **Täglich (Sommerzeit wird nicht unterstützt)** 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 des Geräts veranlassen kann. Es wird empfohlen, einen optimalen Zeitplan der Aufgabe basierend auf den im Unternehmen geltenden Dienstvorschriften zu konfigurieren.

Eine detaillierte Beschreibung der Einstellungen für das Starten nach Zeitplan finden Sie in den allgemeinen Aufgabeneinstellungen.

Anzeigen von Informationen zu verfügbaren Software-Updates von Drittanbietern

Sie können die Liste der verfügbaren Updates für Software von Drittanbietern, einschließlich Microsoft, die auf Client-Geräten installiert ist, anzeigen.

Um die Liste der verfügbaren Updates für die auf den Client-Geräten installierten Programme von Drittanbietern anzuzeigen, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Software-Updates**.

Eine Liste der verfügbaren Updates wird angezeigt.

Sie können einen Filter angeben, um die Liste der Software-Updates anzuzeigen. Klicken Sie in der Liste der Software-Updates auf das Symbol **Filter** (), 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.

Um sich die Eigenschaften eines Updates anzusehen:

1. Klicken Sie auf den Namen des gewünschten Software-Updates.
2. Daraufhin wird das Eigenschaftenfenster des Updates geöffnet, welches die in den folgenden Registerkarten gruppierte Informationen anzeigt:

   - **Allgemein**

     Die Registerkarte zeigt allgemeine Informationen über das ausgewählte Update an:

     - 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
     - Installationsbedingungen, die vom Update vorgeschriebene werden
     - Programmfamilie, zu der das Update gehört
     - Programm, zu dem das Update gehört
     - Revisionsnummer des Updates

   - **Attribute**

Diese Registerkarte zeigt eine Zusammenstellung von Eigenschaften des Updates an, die Sie verwenden können, um weitere Informationen über das Update zu erhalten. Die Zusammenstellung unterscheidet sich dabei je nachdem, ob es sich um ein Update von Microsoft oder von einem Drittthersteller handelt.

Für ein Update von Microsoft zeigt die Registerkarte die folgenden Informationen an:

- Ereignisstufe des Updates, entsprechend dem Microsoft Security Response Center (MSRC)
- Link zu dem Artikel in der Microsoft Wissensdatenbank, in dem das Update beschrieben ist
- Link zu dem Artikel in dem Microsoft Security Bulletin, in dem das Update beschrieben ist
- Update-Identifikator (ID)

Für ein Update eines Drittherstellers zeigt die Registerkarte die folgenden Informationen an:

- Ob das Update ein Patch oder ein vollständiges Programmpaket darstellt
- Lokalisierungssprache des Updates
- On das Update automatisch oder manuell installiert wird
- Ob das Update nach dessen Genehmigung widerrufen wurde
- Link zum Download des Updates

- **Geräte**

  Diese Registerkarte zeigt eine Liste mit den Geräten an, auf denen das ausgewählte Update installiert wurde.

- **Zu schließende Schwachstellen**

  Diese Registerkarte zeigt eine Liste mit Schwachstellen an, die das ausgewählte Update schließen kann.

- **Überschneidungen von Updates**

  Diese Registerkarte zeigt Überschneidungen von verschiedenen, für das gleiche Programm veröffentlichten Updates an. Das heißt, ob das Update entweder 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 zeigt eine Liste mit den Aufgaben an, deren Aufgabenbereiche die Installation des ausgewählten Updates enthalten. Die Registerkarte ermöglicht es Ihnen außerdem, eine neue Aufgabe zur Remote-Installation für das Update zu erstellen.

Um die Statistik einer Updateinstallation anzuzeigen, gehen Sie wir folgt vor:

1. Aktivieren Sie das Kontrollkästchen neben dem gewünschten Softwareupdate.
2. Klicken Sie auf die Schaltfläche **Statistik über die Statuszustände der Update-Installation**.

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 Software-Updates von Drittanbietern, einschließlich Microsoft, die auf dem ausgewählten verwalteten Windows-Gerät installiert ist, anzeigen.

Um eine Liste der verfügbaren Updates für Software von Drittanbietern, die auf dem ausgewählten verwalteten Gerät installiert ist, anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete 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 Software-Updates von Drittanbietern 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 **Verfügbare Updates**. Wenn Sie nur installierte Updates anzeigen möchten, aktivieren Sie die Option **Installierte Updates anzeigen**.

Die Liste der verfügbaren Software-Updates von Drittanbietern für das ausgewählte Gerät wird angezeigt.

Liste der verfügbaren Software-Updates in eine Datei exportieren

Sie können die Liste der Updates für Drittanbieter-Software, einschließlich Microsoft-Software, in eine csv- oder txt-Datei exportieren. Diese Dateien können Sie beispielsweise an Ihren Information Security Manager senden oder zu Statistikzwecken speichern.

Um die Liste der verfügbaren Updates für die Drittanbieter-Programme, die auf allen verwalteten Geräten installiert sind, in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Software-Updates**.

   Eine Liste der verfügbaren Updates wird angezeigt.

   Wenn Sie eine vollständige Liste der Software-Updates exportieren möchten, werden nur die auf der aktuellen Seite angezeigten 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 bevorzugt wird. 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-Software, einschließlich Microsoft-Software, wird auf Ihr aktuelles Gerät heruntergeladen.

Um die Liste der verfügbaren Updates für die Drittanbieter-Programme, die auf dem ausgewählten verwalteten Gerät installiert sind, in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie die Liste der auf dem verwalteten Gerät verfügbaren Drittanbieter-Software-Updates.

   Eine Liste der verfügbaren Updates wird angezeigt.

Wenn Sie eine vollständige Liste der Software-Updates exportieren möchten, werden nur die auf der aktuellen Seite angezeigten 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 bevorzugt wird. 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 die auf dem ausgewählten Gerät installierte Drittanbieter-Software, einschließlich Microsoft-Software, wird auf Ihr aktuelles Gerät heruntergeladen.

Genehmigen und Ablehnen der Software-Updates von Drittanbietern

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 von den 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 Installation der Updates ist effizient. Für die Verwaltung mehrerer Updates können Sie die Regeln verwenden, die Sie in den Eigenschaften der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* 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 große Anzahl von Updates manuell genehmigen, verringert sich die Leistung des Administrationsservers, was zu einer Überlastung des Administrationsservers führen kann.

Um ein oder mehrere Updates zu genehmigen oder abzulehnen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **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 die Schaltfläche **Genehmigen**, um die ausgewählten Updates zu genehmigen, oder auf die Schaltfläche **Ablehnen**, um die ausgewählten Updates abzulehnen. 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.

   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.

Um ein Update in seinen Eigenschaften zu genehmigen oder abzulehnen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **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 entweder 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 für Software-Updates von Drittanbietern den Status *Abgelehnt* angeben, werden die Updates nicht auf den Geräten installiert, auf denen sie vorgesehen waren, aber auf denen sie noch nicht installiert wurden. Auf den Geräten, auf denen die Updates bereits installiert wurden, bleiben diese auch weiterhin. 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 unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* wird verwendet, um Schwachstellen in Software von Drittanbietern, die auf verwalteten Geräten installiert ist, zu aktualisieren und zu beheben. Mit dieser Aufgabe können Sie mehrere Updates installieren und mehrere Schwachstellen gemäß den Regeln schließen, die Sie in den Aufgabeneinstellungen festlegen.

Sie haben eine der folgenden Möglichkeiten, um mithilfe der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* Updates zu installieren oder Schwachstellen zu schließen:

- Führen Sie den Assistenten zur Installation von Updates oder den Assistenten zum Schließen von Schwachstellen aus.
- Erstellen einer Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen*.
- Fügen Sie eine Regel zur Installation von Updates 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 **Assets (Geräte)** → **Aufgaben**.

2. Klicken Sie auf die Schaltfläche **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 **Programm** 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. Sie könne die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* ohne diese Zugriffsrechte nicht erstellen und konfigurieren.

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.

7. Geben Sie im 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 übernommen. Wenn keine Regeln festgelegt sind, hat die Aufgabe nichts auszuführen. 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, kann die Aufgabe nichts ausführen.

8. Geben Sie die folgenden Einstellungen an:

   - **Installation beim Neustart bzw. beim Herunterfahren des Geräts beginnen**

     Wenn diese Option aktiviert ist, werden Updates installiert, wenn das Gerät neu gestartet oder heruntergefahren wird. Anderenfalls werden Updates gemäß einem Zeitplan installiert.

     Verwenden Sie diese Option, wenn die Installation von Updates die Leistung des Geräts 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 neue Programmversionen für Updates zulassen**

Wenn diese Option aktiviert ist, 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 eine Aktualisierung in einer Testinfrastruktur überprüfen möchten.

Diese Option ist standardmäßig aktiviert.

Aktualisieren 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 von Drittanbieter-Apps (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden) werden in den Ordner heruntergeladen, der im Feld **Updates laden 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 von Drittanbieter-Apps (Anwendungen, die von anderen Programmherstellern als Kaspersky und Microsoft entwickelt wurden) herunterzuladen.

- Erweiterte Diagnose aktivieren

Wenn diese Funktion aktiviert ist, führt der Administrationsagent die Ablaufverfolgung auch dann durch, wenn die Ablaufverfolgung für den Administrationsagenten im Tool zur 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, beginnt der Administrationsagent sie wieder von vorn zu überschreiben. Die Ablaufverfolgungsdateien werden im Ordner %WINDIR%\Temp gespeichert. Auf diese Dateien kann im Tool zur Remote-Diagnose zugegriffen werden, dort können Sie diese herunterladen oder löschen.

Wenn diese Funktion deaktiviert ist, führt der Administrationsagent die Ablaufverfolgung gemäß den Einstellungen im Tool zur Remote-Diagnose für Kaspersky Security Center Linux durch. Es erfolgt keine zusätzliche Ablaufverfolgung.

Beim Erstellen einer Aufgabe, müssen Sie die erweiterte Diagnose nicht aktivieren. Sie möchten diese Funktion möglicherweise später verwenden, beispielsweise, wenn eine Aufgabe auf einigen Geräten fehlschlägt und Sie während einer weiteren Aufgabenausführung zusätzliche Informationen empfangen möchten.

Diese Option ist standardmäßig deaktiviert.

  - Maximale Größe der Dateien für die erweiterte Diagnose (MB)

Der Standardwert beträgt 100 MB und verfügbare Werte liegen zwischen 1 MB und 2048 MB. Sie werden möglicherweise von einem Experten des Technischen Supports von Kaspersky gebeten, den Standardwert zu ändern, wenn die Informationen in den von Ihnen gesendeten Dateien für die erweiterte Diagnose nicht ausreichen, um das Problem zu beheben.

Wechseln Sie zum nächsten Schritt des Assistenten.

9. Geben Sie Neustart-Einstellungen des Betriebssystems an:

- **Gerät nicht neu starten**

  Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) 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 Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

- **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

- **Benutzer fragen**

  Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. 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. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten 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.

- **Wartezeit vor dem erzwungenen Schließen von Programmen in gesperrten Sitzungen (Min.)**

  Erzwungenes Schließen der Programmausführung, wenn das Gerät des Benutzers gesperrt ist (automatisch nach einer Phase der Inaktivität oder manuell).

  Wenn diese Option aktiviert ist, werden die Programme auf einem gesperrten Gerät nach Ablauf der im Eingabefeld angegebenen Zeitspanne automatisch geschlossen.

  Wenn diese Option deaktiviert ist, werden die Programme auf einem gesperrten Gerät nicht geschlossen.

  Diese Option ist standardmäßig deaktiviert.

10. 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.

11. Klicken Sie auf die Schaltfläche **Fertigstellen**.

    Der Assistent Assistent für das Erstellen einer Aufgabe 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 bei der Aufgabenerstellung festgelegten Einstellungen ändern.

    Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Liste mit Aufgaben auf den Namen der erstellten Aufgabe klicken.

    Die Aufgabe ist erstellt, konfiguriert und wird in der Aufgabenliste angezeigt.

12. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf die Schaltfläche **Starten**.

    Sie können auf der Registerkarte **Zeitplan** im Eigenschaftenfenster der Aufgabe auch einen Zeitplan für den Aufgabenstart festlegen.

    Eine detaillierte Beschreibung der Einstellungen für das Starten nach Zeitplan finden Sie in den allgemeinen Aufgabeneinstellungen.

Nach Abschluss der Aufgabe wurden die erforderlichen Updates installiert und die Schwachstellen geschlossen.

Hinzufügen einer Regel für die Installation von Updates

Diese Funktion ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Bei der Installation von Software-Updates oder dem Schließen von Schwachstellen in Programmen mithilfe 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 von Windows Update oder für Updates von Drittanbieter-Programmen (Programme von anderen Softwareherstellern als Kaspersky und Microsoft) hinzufügen. Beim Hinzufügen einer Regel für Updates von Windows Update oder Updates von Drittanbieter-Programmen 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 mittels Installation von Updates schließen möchten, auswählen.

Sie können eine Regel für die Update-Installation 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 **Programmeinstellungen** in den Aufgabeneigenschaften einer bestehenden Aufgabe des Typs *Erforderliche Updates installieren und Schwachstellen schließen*.
- Durch Ausführen des Assistenten zur Installation von Updates oder des Assistenten zum Schließen von Schwachstellen.

Regeln für alle Updates hinzufügen

Um eine neue Regel für alle Updates hinzuzufügen, gehen Sie wie folgt vor:

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:

   - **Menge 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 von ihrem 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 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 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.

Wechseln Sie zum nächsten Schritt des Assistenten.

4. Auswählen der zu installierenden Updates

- **Alle relevanten Updates installieren**

  Installieren Sie alle Software-Updates, welche die Kriterien des Schrittes **Allgemeine Kriterien** des Assistenten erfüllen. Standardmäßig ausgewählt.

- **Nur Updates aus der Liste installieren**

  Es werden nur Software-Updates installiert, die Sie manuell aus der Liste auswählen. Diese Liste enthält alle verfügbaren Software-Updates.

  Sie können beispielsweise in den folgenden Fällen bestimmte Updates auswählen: um deren Installation in einer Testumgebung zu überprüfen, um nur kritische Apps zu aktualisieren oder um nur bestimmte Programme zu aktualisieren.

  - **Alle vorherigen Programm-Updates, die für die Installation der ausgewählten Updates erforderlich sind, automatisch installieren**

    Lassen Sie diese Option optimiert, wenn Sie mit der Installation von Programmzwischenversionen einverstanden sind, wenn 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 eine geradlinige Weist 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.

    Wenn Sie beispielsweise Version 3 eines Programms auf einem Gerät installiert haben und Sie es auf Version 5 aktualisieren möchten, Version 5 dieses Programms aber nur über Version 4 installiert werden kann. 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.

Wechseln 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 deren Schließen in einer Testumgebung zu überprüfen, um Schwachstellen nur in kritischen Apps zu schließen oder um Schwachstellen nur in bestimmten Programmen zu aktualisieren.

Wechseln Sie zum nächsten Schritt des Assistenten.

6. Geben Sie den Namen für die hinzuzufügende Regel an. Sie können diesen Namen später in der Registerkarte **Programmeinstellungen** 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 von Windows Update hinzufügen

So fügen Sie eine neue Regel für Updates von 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.

   Wechseln Sie zum nächsten Schritt des Assistenten.

3. Geben Sie im Schritt **Allgemeine Kriterien** des Assistenten die folgenden Einstellungen an:

   - Satz 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 von ihrem 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 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 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 **Apps** die Apps und Programmversionen aus, für die Sie Updates installieren möchten. Standardmäßig sind alle Programme ausgewählt.

5. Wählen Sie auf der Seite **Update-Kategorien** die Kategorien von Updates aus, die installiert werden sollen. Diese Kategorien sind dieselben wie 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 das Erstellen einer Regel wird die neue Regel hinzugefügt und in der Regelliste im Assistenten für das Erstellen einer Aufgabe oder in den Aufgabeneigenschaften angezeigt.

Regeln für Updates von Drittanbieter-Programmen hinzufügen

Um eine neue Regel für Updates von Drittanbieter-Programmen hinzuzufügen, gehen Sie wie folgt vor:

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:

   - Satz 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 von ihrem 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 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 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.

Wechseln 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.

   Wechseln Sie zum nächsten Schritt des Assistenten.

5. Geben Sie den Namen für die hinzuzufügende Regel an. Sie können diesen Namen später in der Registerkarte **Programmeinstellungen** 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 **Programmeinstellungen** 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 prüfen möchten. Klicken Sie auf die Schaltfläche **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 prüfen 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 prüfen möchten. Geben Sie im Feld **Prozentualer Anteil der Testgeräte an der Gesamtanzahl von Zielgeräten** den Prozentanteil der Geräte an, auf denen Sie die Testinstallation von Updates ausführen möchten.

  Sobald Sie eine beliebige Option gewählt haben (mit Ausnahme von **Nicht untersuchen**), geben Sie im Feld **Zeitraum in Stunden, um zu entschieden, ob die Installation fortgesetzt wird** die Anzahl an Stunden an, die nach der Testinstallation der Updates und vor dem Beginn der Installation der Updates auf allen weiteren Geräten vergehen sollen.

- Im Abschnitt **Zu installierende Updates** können Sie die Liste der bei der Aufgabe installierten Updates angezeigt. 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-Programme können automatisch aktualisiert werden. Der Hersteller des jeweiligen Programms legt fest, ob das Programm die Auto-Update-Funktion unterstützt. Wenn das auf einem verwalteten Gerät installierte Drittanbieter-Programm Auto-Update unterstützt, können Sie die Auto-Update-Einstellungen in den Programmeinstellungen konfigurieren. Nach dem Ändern der Auto-Update-Einstellungen, wenden die Administrationsagenten die neuen Einstellungen auf jedes verwaltete Gerät an, auf dem das Programm installiert ist.

Die Auto-Update-Einstellung ist von den anderen Objekten und Einstellungen der Funktionen für Schwachstellen- und Patch-Management unabhängig. So hängt diese Einstellung beispielsweise nicht vom Genehmigungsstatus eines Updates oder von den Aufgaben zur Update-Installation, wie *Erforderliche Updates installieren und Schwachstellen schließen* und *Schwachstellen schließen*, ab.

Um die Auto-Update-Einstellung für ein Drittanbieter-Programm zu konfigurieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry**.

2. Klicken Sie auf den Namen des Programms, für das Sie die Auto-Update-Einstellung ändern wollen.

   Um die Suche zu erleichtern, können Sie Liste mittels den 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-Programme unter Verwendung der Aufgaben *Erforderliche Updates installieren und Schwachstellen schließen* und *Schwachstellen schließen*.

- **Zugelassen**

  Nachdem der Hersteller für das Programm ein Update veröffentlicht hat, wird dieses 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-Programme 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-Einstellungen werden auf das ausgewählte Programm angewendet.

Schließen von Schwachstellen in Programmen von Drittanbietern

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 installierten 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 Software von Drittanbietern, einschließlich Microsoft-Software, erkannt.

Finden von Schwachstellen in Programmen

Kaspersky Security Center Linux verwendet Merkmale aus der Datenbank mit bekannten Schwachstellen, um Schwachstellen in Programmen zu finden. Diese Datenbank wurde von den Experten bei Kaspersky erstellt und wird fortlaufend aktualisiert. Sie enthält Informationen zu Schwachstellen, z. B. eine Beschreibung, das Datum der Erkennung und die Signifikanz der Schwachstelle. Informationen über Schwachstellen in Programmen finden Sie auf der Website von Kaspersky.

Kaspersky Security Center Linux verwendet die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*, um Schwachstellen in Programmen zu finden.

Beheben von Schwachstellen in Programmen

Zum Beheben von Schwachstellen in Programmen verwendet Kaspersky Security Center Linux die Software-Updates der Programmhersteller. Die Metadaten der Software-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- und Drittanbieter-Software herunterzuladen. Diese Aufgabe wird vom Schnellstartassistent des Kaspersky Security Centers Linux automatisch erstellt. Sie können die Aufgabe *Download von Updates in die Datenverwaltung des Administrationsservers* manuell erstellen.

Software-Updates zur Behebung von Schwachstellen können in Form von vollständigen Programmpaketen oder Patches bereitgestellt werden. Software-Updates, die Schwachstellen in Programmen beheben, werden als *Korrekturen* bezeichnet. *Empfohlene Korrekturen* sind solche, deren Installation von Kaspersky-Spezialisten empfohlen wird. *Benutzerdefinierte Korrekturen* sind solche, die manuell für die Installation durch Benutzer ausgewählt werden. Um eine Benutzerkorrektur 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 Microsoft-Programme und benutzerdefinierte Korrekturen für andere Programme von Drittanbietern installiert werden.

Aus Sicherheitsgründen werden alle Software-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 Prüfung von Dateien verwendet und umfassen die Untersuchung auf Viren, die statische und die dynamische Analyse, die Verhaltensanalyse in der Sandbox-Umgebung, sowie Machine Learning.

Kaspersky-Experten führen keine manuelle Analyse von Software-Updates von Drittanbietern 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 im obigen Abschnitt genannten hinausgehen.

Eine Benutzerinteraktion kann erforderlich sein, 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.

Zum Schließen bestimmter Schwachstellen in Programmen müssen Sie den Endbenutzer-Lizenzvertrag (EULA) für die Installation der Software akzeptieren, wenn dies angefordert wird. 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 Microsoft-Programmen, 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 Microsoft-Software. Die Liste wird von Kaspersky-Spezialisten erstellt und regelmäßig aktualisiert.
  - Beheben von Schwachstellen in anderer Software von Drittanbietern als Microsoft-Software.

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 installierte Software von Drittanbietern, 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 Software von Drittanbietern, einschließlich 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 Software-Updates.

   Die Aufgabe *Schwachstellen schließen* erfordert keine Lizenz-Option für die Funktion "Schwachstellen- und Patch-Management". Um die Aufgabe zu verwenden, müssen Sie manuell Benutzerdefinierte Korrekturen angeben, um die Schwachstellen in Programmen von Drittanbietern zu beheben, die in den Aufgabeneinstellungen aufgeführt sind. Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für Microsoft-Programme und die benutzerdefinierten 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 zum 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 Software-Updates mit den Regeln abgeglichen, die in den Aufgabeneinstellungen angegeben sind. Alle Software-Updates, welche die Kriterien der angegebenen Regeln erfüllen, 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 Programmen von Microsoft behoben.

4. **Planen der Aufgaben**

   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 Microsoft-Programme auswählen oder benutzerdefinierte Korrekturen für Drittanbieterprogramme 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 Programme von Drittanbietern, einschließlich Microsoft, die in Ihrem Unternehmen verwendet werden, Schwachstellen zu identifizieren und zu beheben.

8. **Überprüfen der Konfiguration zum Finden und Schließen von Schwachstellen in Programmen von Drittanbietern**

   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.

Schließen von Schwachstellen in Programmen von Drittanbietern

Um Schwachstellen in Programmen von Drittanbietern zu finden, können Sie die Aufgabe *Suche nach Schwachstellen und erforderlichen Updates* erstellen und ausführen, um eine Liste mit Schwachstellen in Programmen zu erhalten. Nachdem Sie die Liste mit den Schwachstellen in Programmen abgerufen haben, können Sie die Schwachstellen auf den verwalteten Windows-Geräten beheben.

Das Schließen von Schwachstellen in Programmen im Betriebssystem und in Software von Drittanbietern, einschließlich Microsoft-Software, ist mithilfe der Aufgaben Schwachstellen schließen oder Erforderliche Updates installieren und Schwachstellen schließen möglich.

Eine Benutzerinteraktion kann erforderlich sein, 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 Schwachstellen in Programmen auf folgende Weise zu schließen:

- Öffnen Sie die Schwachstellenliste und geben Sie an, welche Schwachstellen geschlossen werden sollen.

  Infolgedessen wird eine neue Aufgabe zum Schließen von Schwachstellen in Programmen erstellt. Optional können Sie die ausgewählten Schwachstellen einer existierenden Aufgabe hinzufügen.

- Führen Sie den Assistenten zum Schließen von Schwachstellen aus.

  Der Assistent zum Schließen von Schwachstellen ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

  Der Assistent vereinfacht die Erstellung und Konfiguration einer Aufgabe zum Schließen von Schwachstellen und ermöglicht es Ihnen, die Erstellung redundanter Aufgaben zu vermeiden.

Schließen von Schwachstellen in Programmen mithilfe der Schwachstellenliste

So schließen Sie Schwachstellen in Programmen mithilfe der Schwachstellenliste:

1. Öffnen Sie die Schwachstellenliste, indem Sie einen der folgenden Schritte ausführen:
   - Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.
   - Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete Geräte** → <Gerätename> → **Erweitert** → **Schwachstellen in Programmen**.
   - Wechseln Sie im Hauptmenü zu **Vorgänge** → **Drittanbieter-Programme** → **Programm-Registry** → <Programmname> → **Schwachstellen**.

   Eine Tabelle mit der Liste von Schwachstellen in Programmen von Drittanbietern, die auf den verwalteten Geräten installiert sind, wird angezeigt.

2. Aktivieren Sie in der Liste der Schwachstellen die Kontrollkästchen neben den Schwachstellen, die Sie schließen möchten, und klicken Sie anschließend auf die Schaltfläche **Schwachstelle schließen**.

   Wenn das empfohlene Update zum Schließen der Schwachstelle nicht vorhanden ist, wird dies gemeldet.

   Zum Schließen bestimmter Schwachstellen in Programmen müssen Sie die Endbenutzer-Lizenzvertrag (EULA) für die Installation der Software akzeptieren, wenn dies angefordert wird. 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, wird die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen vorausgewählt. Wenn Sie nicht über die Lizenz verfügen, wird 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 nicht über die Lizenz verfügen, 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 in der Aufgabenliste unter **Assets (Geräte)** → **Aufgaben** angezeigt. Wenn Sie sich entschieden haben, die Schwachstellen zu einer existierenden Aufgabe hinzuzufügen, werden die Schwachstellen in den Aufgabeneigenschaften gespeichert.

Um Schwachstellen in Programmen von Drittanbietern 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 die in den Aufgabeneinstellungen aufgelisteten Software-Updates manuell angeben.

Schließen von Schwachstellen in Programmen mithilfe des Assistenten zum Schließen von Schwachstellen

Der Assistent zum Schließen von Schwachstellen ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

Um Schwachstellen in Programmen mithilfe des Assistenten zum Schließen von Schwachstellen zu beheben, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

   Eine Tabelle mit einer Liste von Schwachstellen in Programmen von Drittanbietern, 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 die Schaltfläche **Assistent zum Schließen von Schwachstellen starten**.

Die Schaltfläche ist deaktiviert, wenn Sie mehr als eine Schwachstelle auswählen.

Der Assistent zum 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 soll, 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 die Schaltfläche **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 die Schaltfläche **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 sich öffnenden Seite die neue Regel:

     - Regel zum Schließen aller Schwachstellen der ausgewählten Signifikanz

       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 von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Schweregrad des ausgewählten Updates (**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.

     - **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 Microsoft-Software angezeigt.

- **Regel zum Schließen von Schwachstellen in Programmen des ausgewählten Anbieters**

  Diese Regel wird nur für Schwachstellen in Drittanbieter-Software angezeigt.

- **Regel zum Schließen von Schwachstellen in allen Versionen des ausgewählten Programms**

  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 bereits 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 die Schaltfläche **Neue Aufgabe**.

b. Konfigurieren Sie auf der sich öffnenden Seite die neue Regel:

- Regel zum Schließen aller Schwachstellen der ausgewählten Signifikanz

  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 von Kaspersky festgelegte Signifikanz gleich oder höher ist als der Schweregrad des ausgewählten Updates (**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.

- **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 Microsoft-Software angezeigt.

- **Regel zum Schließen von Schwachstellen in Programmen des ausgewählten Anbieters**

  Diese Regel wird nur für Schwachstellen in Drittanbieter-Software angezeigt.

- **Regel zum Schließen von Schwachstellen in allen Versionen des ausgewählten Programms**

  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 Assistent zum Schließen von Schwachstellen hinzugefügt haben, wird im Schritt **Regeln für die Installation von Updates festlegen** des Assistenten für das Erstellen einer Aufgabe angezeigt. Wenn Sie den Assistenten abgeschlossen haben, wurde die Aufgabe Erforderliche Updates installieren und Schwachstellen schließen der Aufgabenliste hinzugefügt.

Erstellen der Aufgabe "Schwachstellen schließen"

Die Aufgabe *Schwachstellen schließen* ermöglicht das Schließen von Schwachstellen in Programmen auf verwalteten Geräten. Sie können Schwachstellen in Programmen in den Programmen von Drittanbietern, einschließlich 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 eine neue Aufgabe des Typs *Schwachstellen schließen* nur dann erstellen, wenn Sie über die Lizenz für das Schwachstellen- und Patch-Management verfügen.

Wenn Sie über die Lizenz für Schwachstellen- und Patch-Management verfügen, können Sie keine neuen Aufgaben des Typs *Schwachstellen schließen* erstellen. Um neue Schwachstellen zu schließen, können Sie diese zu einer bestehenden Aufgabe des Typs *Schwachstellen schließen* hinzufügen. Wir empfehlen jedoch die Verwendung der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* statt der Aufgabe *Schwachstellen schließen*. Die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* ermöglicht es Ihnen, mehrere Updates zu installieren und mehrere Schwachstellen automatisch gemäß den von Ihnen definierten Regeln zu schließen.

Eine Benutzerinteraktion kann erforderlich sein, 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 **Assets (Geräte)** → **Aufgaben**.

Alternativ können Sie diese Aufgabe auch im Eigenschaftenfenster des Geräts auf der Registerkarte **Aufgaben** erstellen.

2. Klicken Sie auf die Schaltfläche **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 **Programm** 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 die Schaltfläche **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 die Schaltfläche **OK**.

   Schwachstellen in Programmen von Microsoft haben normalerweise empfohlene Korrekturen. Für sie sind keine zusätzlichen Aktionen erforderlich.

   Bei Schwachstellen in Software anderer Anbieter müssen Sie zunächst einen Benutzer-Fix für jede Schwachstelle angeben, die Sie schließen möchten. Danach können Sie diese Schwachstellen der Aufgabe *Schwachstellen schließen* hinzufügen.

   Wechseln Sie zum nächsten Schritt des Assistenten.

9. Geben Sie Neustart-Einstellungen des Betriebssystems an:

   - **Gerät nicht neu starten**

     Client-Geräte werden nach dem Vorgang nicht automatisch neu gestartet. Für das Abschließen des Vorgangs ist es erforderlich, ein Gerät (beispielsweise manuell oder mithilfe einer Aufgabe zur Verwaltung von Geräten) 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 Aufgaben auf Servern und anderen Geräten, für welche ein störungsfreies Arbeiten kritisch ist.

   - **Gerät 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, für die regelmäßige Pausen in der Ausführung (Deaktivieren, Neustart) zulässig sind.

   - **Benutzer fragen**

Die Erinnerung an den Neustart wird auf dem Bildschirm des Client-Geräts angezeigt und fordert den Benutzer auf, das Gerät manuell neu zu starten. 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. Diese Option eignet sich am besten für Workstations, an denen Benutzer in der Lage sein müssen, den passendsten 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. Verfügbare Werte liegen zwischen 1 und 1.440 Minuten.

  Wenn diese Option deaktiviert ist, wird die Aufforderung nur ein einziges Mal angezeigt.

- **Neu starten 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 das Neustarten des Client-Geräts verhindern. Wenn beispielsweise ein Dokument in einer Textverarbeitungsanwendung bearbeitet wird und nicht gespeichert wurde, erlaubt die Anwendung keinen Neustart des Geräts.

  Wenn diese Option aktiviert ist, wird das Schließen solcher Anwendungen auf einem gesperrten Gerät erzwungen, bevor das Gerät neu gestartet wird. Das kann dazu führen, dass Benutzer ihre nicht gespeicherten 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.

Wechseln Sie zum nächsten Schritt des Assistenten.

10. Legen Sie die Benutzerkonto-Einstellungen fest:

- **Standardbenutzerkonto**

  Die Aufgabe wird unter demselben Benutzerkonto ausgeführt, unter dem das Programm installiert und gestartet wurde, dass diese Aufgabe ausführt.

  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 dessen Namen die Aufgabe ausgeführt wird.

- **Kennwort**

  Kennwort des Benutzerkontos, unter dessen Namen die Aufgabe gestartet wird.

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 **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 bei der Aufgabenerstellung festgelegten Einstellungen ändern.

    Sie können das Fenster mit den Aufgabeneigenschaften auch öffnen, indem Sie in der Liste mit Aufgaben auf den Namen der erstellten Aufgabe klicken.

    Die Aufgabe ist erstellt, konfiguriert und wird in der Aufgabenliste unter **Assets (Geräte)→ Aufgaben** angezeigt.

13. Um die Aufgabe auszuführen, wählen Sie diese in der Aufgabenliste aus und klicken Sie anschließend auf die Schaltfläche **Starten**.

    Sie können auf der Registerkarte **Zeitplan** im Eigenschaftenfenster der Aufgabe auch einen Zeitplan für den Aufgabenstart festlegen.

    Eine detaillierte Beschreibung der Einstellungen für das Starten 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

Um die Aufgabe *Schwachstellen schließen* zu verwenden, müssen Sie die Software-Updates manuell angeben, um die Schwachstellen in den Drittanbieter-Programmen zu beheben, die in den Aufgabeneinstellungen aufgeführt sind. Die Aufgabe *Schwachstellen schließen* verwendet die empfohlenen Korrekturen für Microsoft-Programme und die benutzerdefinierten Korrekturen für andere Drittanbieter-Programme.

Benutzerdefinierte Korrekturen sind Software-Updates, die der Administrator manuell zur Installation angibt, um Schwachstellen zu schließen.

So wählen Sie benutzerdefinierte Korrekturen für Schwachstellen in Software von Drittanbietern aus:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

   Eine Tabelle mit der Liste von Schwachstellen in Programmen von Drittanbietern, die auf den verwalteten Geräten installiert sind, wird angezeigt.

2. Klicken Sie in der Liste der Schwachstellen in Programmen auf den Link mit dem Namen der Software-Schwachstelle, für die Sie eine Benutzerkorrektur angeben möchten.

   Das Eigenschaftenfenster der gewählten Schwachstelle wird geöffnet.

3. Wählen Sie im linken Fensterbereich den Abschnitt **Benutzerdefinierte und andere Patches**.

   Die Liste der benutzerdefinierten Korrekturen für die ausgewählte Software-Schwachstelle wird angezeigt.

4. Klicken Sie auf die Schaltfläche **Hinzufügen**.

   Eine Liste der verfügbaren Installationspakete wird angezeigt. Die Liste der angezeigten Installationspakete entspricht der Liste unter **Vorgänge** → **Datenverwaltung** → **Installationspakete**.

   Wenn Sie kein Installationspaket erstellt haben, das eine benutzerdefinierte Korrektur für die ausgewählte Schwachstelle enthält, können Sie das Paket jetzt erstellen, indem Sie auf die Schaltfläche **Neu** anklicken und dem Assistenten für das Erstellen eines Installationspakets folgen.

5. Wählen Sie ein Installationspaket (bzw. Pakete) aus, in dem eine benutzerdefinierte Korrektur (bzw. benutzerdefinierte Korrekturen) für die ausgewählte Schwachstelle enthalten ist.

6. Klicken Sie auf die Schaltfläche **Speichern**.

Die Installationspakete, die benutzerdefinierte Korrekturen für die Software-Schwachstelle enthalten, werden angegeben. Wenn Sie die Aufgabe *Schwachstellen schließen* starten, wird das Installationspaket installiert und die Schwachstelle in der Software geschlossen.

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 Schwachstellen in Programmen anzeigen. Sie können auch Bericht über Schwachstellen erstellen und anzeigen.

Um eine Liste mit Schwachstellen in Programmen, die auf den verwalteten Geräten erkannt wurden, anzuzeigen, gehen Sie wie folgt vor:

Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

Die Liste der Schwachstellen in Programmen, die auf dem Client-Gerät erkannt wurden, wird angezeigt.

So passen Sie die Liste der Schwachstellen in Programmen an:

Klicken Sie auf das Symbol **Filter** () oben rechts in der Liste mit Schwachstellen in Programmen und wählen Sie den erforderlichen Filter aus. Sie können auch einen der voreingestellten Filter aus der Dropdown-Liste **Vordefinierte Filter** oberhalb der Liste mit Schwachstellen in Programmen auswählen.

Sie können ausführliche Informationen über Schwachstellen über die Liste abrufen.

So rufen Sie Informationen über eine Schwachstelle in einem Programmen ab:

Klicken Sie in der Liste mit Schwachstellen in Programmen auf den Link mit dem Namen der Schwachstelle.

Das Eigenschaftenfenster der Schwachstelle im Programm wird geöffnet.

Anzeigen von Informationen zu Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden

Sie können Informationen zu Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Windows-Gerät erkannt wurden, anzeigen.

Um eine Liste mit den Schwachstellen in Programmen auf dem ausgewählten verwalteten Gerät zu exportieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete 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 Schwachstellen in Programmen 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**.

   Die Liste der Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden, wird angezeigt.

Um Eigenschaften der ausgewählten Schwachstelle anzuzeigen, gehen Sie wie folgt vor:

Klicken Sie in der Liste der Schwachstellen in Programmen auf den Link mit dem Namen der Schwachstelle.

Das Eigenschaftenfenster der gewählten Schwachstelle wird geöffnet.

Anzeigen von Statistiken zu Schwachstellen auf verwalteten Geräten

Sie können Statistiken für jede Schwachstelle in Programmen auf verwalteten Geräten anzeigen. Die Statistik wird als Diagramm dargestellt. Das Diagramm zeigt die Anzahl der Geräte mit den folgenden Status an:

- *Ignoriert auf: <Anzahl der Geräte>*. Dieser Status wird zugewiesen, wenn Sie in den Eigenschaften der Schwachstelle die Option zum Ignorieren der Schwachstelle manuell 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, sie jedoch noch nicht ausgeführt wurde.
- *Patch angewendet auf: <Anzahl der Geräte>*. Der Status wird zugewiesen, wenn Sie ein 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.

Um die Statistiken zur Schwachstelle auf einem verwalteten Gerät anzuzeigen, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

   Die Seite zeigt eine Liste der Schwachstellen für die Programmen an, die auf den verwalteten Geräten erkannt wurden.

2. Aktivieren Sie das Kontrollkästchen neben einer Schwachstelle.

3. Klicken Sie auf die Schaltfläche **Statistik zu Schwachstellen auf Geräten**.

   > Die Schaltfläche **Statistik zu Schwachstellen auf Geräten** ist deaktiviert, wenn Sie mehr als eine Schwachstelle auswählen.

   Ein Diagramm der Schwachstellenstatus 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.

Um eine Liste der Schwachstellen in Programmen, die auf allen verwalteten Geräten erkannt wurden, in eine Textdatei zu exportieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

   Es wird eine Liste mit Schwachstellen in Programmen, die auf verwalteten Geräten gefunden wurden, wird angezeigt.

   Standardmäßig werden nur jene Schwachstellen exportiert, die auf der aktuellen Seite angezeigt werden.

   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 bevorzugt wird. 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.

   Eine Datei mit der Liste der Schwachstellen in Programmen wird auf Ihr Gerät heruntergeladen.

Um eine Liste mit den Schwachstellen in Programmen auf dem ausgewählten verwalteten Gerät zu exportieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete 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 Schwachstellen in Programmen 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**.

   Die Liste der Schwachstellen in Programmen, die auf dem ausgewählten verwalteten Gerät erkannt wurden, wird angezeigt.

   Standardmäßig werden nur jene Schwachstellen exportiert, die auf der aktuellen Seite angezeigt werden.

   Wenn Sie nur ausgewählte Schwachstellen exportieren möchten, aktivieren Sie die Kontrollkästchen neben diesen Schwachstellen.

5. Klicken Sie auf **In txt-Datei exportieren** oder **In csv-Datei exportieren**, je nachdem, welches Format bevorzugt wird. 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.

Eine Datei mit der Liste der Schwachstellen in Programmen wird auf Ihr Gerät heruntergeladen.

Ignorieren von Schwachstellen in Programmen

Sie können Korrekturen für Schwachstellen in Programmen ignorieren. Die Gründe für das Ignorieren von Schwachstellen in Programmen können beispielsweise folgende sein:

- Sie betrachten die Schwachstelle im Programm nicht als kritisch für Ihr Unternehmen.
- Sie vermuten, dass durch das Schließen von Schwachstellen in Programmen die Daten des Programms beschädigt werden können, welches das Schließen von Schwachstellen erforderlich macht.
- Sie sind sicher, dass die Schwachstelle im Programm keine Gefahr für das Netzwerk Ihres Unternehmens darstellt, da Sie andere Maßnahmen ergriffen haben, um Ihre verwalteten Geräte zu schützen.

Sie können eine Schwachstelle im Programm auf allen verwalteten Geräten oder nur auf den ausgewählten verwalteten Geräten ignorieren.

Um eine Schwachstelle im Programm auf allen verwalteten Geräten zu ignorieren, gehen Sie wie folgt vor:

1. Wechseln Sie im Hauptmenü zu **Vorgänge** → **Patch-Management** → **Schwachstellen in Programmen**.

   Es wird eine Liste mit Schwachstellen in Programmen, die auf verwalteten Geräten gefunden wurden, wird angezeigt.

2. Klicken Sie in der Liste der Schwachstellen in Programmen auf den Link mit dem Namen der Schwachstelle, die Sie ignorieren möchten.

   Das Fenster mit den Eigenschaften der Schwachstelle im Programm öffnet sich.

3. Aktivieren Sie auf der Registerkarte **Allgemein** die Option **Schwachstelle ignorieren**.

4. Klicken Sie auf die Schaltfläche **Speichern**.

Das Fenster mit den Eigenschaften der Schwachstelle im Programm schließt sich.

Die Schwachstelle im Programm wird auf allen verwalteten Geräten ignoriert.

So ignorieren Sie eine Schwachstelle im Programm auf einem ausgewählten verwalteten Gerät:

1. Wechseln Sie im Hauptmenü zu **Assets (Geräte)** → **Verwaltete 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 Schwachstelle im Programm ignorieren möchten.

   Das Fenster mit den Geräteeigenschaften wird geöffnet.

3. Wählen Sie im Eigenschaftenfenster des Geräts die Registerkarte **Erweitert** aus.

4. Wählen Sie im linken Fensterbereich den Abschnitt **Schwachstellen in Programmen**.

   Die Liste der Schwachstellen in Programmen, die auf dem Gerät erkannt wurden, wird angezeigt.

5. Wählen Sie in der Liste der Schwachstellen in Programmen 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 Schwachstelle im Programm 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 Fenster mit den Geräteeigenschaften.

Die Schwachstelle im Programm wird auf dem ausgewählten Gerät ignoriert.

Die ignorierte Schwachstelle im Programm wird im Rahmen der Aufgabe *Schwachstellen schließen* oder *Erforderliche Updates installieren und Schwachstellen schließen* nicht behoben. Mithilfe eines Filters können Sie ignorierte Schwachstellen in Programmen aus der Liste der Schwachstellen ausschließen.

Erstellen eines Installationspakets eines Drittanbieterprogramms aus der Kaspersky-Datenbank

Mit Kaspersky Security Center Web Console können Sie mithilfe von Installationspaketen eine Remote-Installation von Drittanbieterprogrammen durchführen. Solche Drittanbieterprogramme 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 ein Drittanbieter-Programms aus der Kaspersky-Datenbank erstellen, wenn Sie über eine Lizenz für das Schwachstellen- und Patch-Management verfügen.

So erstellen Sie ein Installationspaket eines Drittanbieterprogramms aus der Kaspersky-Datenbank:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → 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 **Programm aus der Kaspersky-Datenbank auswählen, um ein Installationspaket zu erstellen**.

   > Diese Variante ist nur unter der Lizenz für Schwachstellen- und Patch-Management verfügbar.

   Wechseln Sie zum nächsten Schritt des Assistenten.

4. Wählen Sie das Programm aus, für das Sie eine Installationspaket erstellen möchten.

   Wechseln Sie zum nächsten Schritt des Assistenten.

5. Wählen Sie die erforderliche Spachversion in der Dropdown-Liste aus und klicken Sie anschließend auf Weiter.

   > Dieser Schritt wird nur angezeigt, wenn die Anwendung mehrere Sprachoptionen 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 die Schaltfläche **Alle akzeptieren**, um alle Lizenzvereinbarungen und Datenschutzrichtlinien zu akzeptieren, die in der Liste angezeigt werden.

7. Geben Sie im Schritt **Name des neuen Installationspakets** des Assistenten im Feld **Paketname** den Namen für das Installationspaket ein und klicken anschließend auf **Weiter**.

   Das neu erstellte Installationspaket wird auf den Administrationsserver hochgeladen. Der Assistent für das Erstellen eines Installationspakets zeigt eine Nachricht an, dass das Installationspaket erfolgreich erstellt wurde.

8. Klicken Sie auf die Schaltfläche **Fertigstellen**.

Das neu erstellte Installationspaket wird in der Liste der Installationspakete angezeigt. Sie können dieses Paket auswählen, wenn Sie die Aufgabe *Remote-Installation eines Programms* erstellen oder ändern.

> Sie können die Aufgabe *Remote-Installation eines Programms* nur dann unter Verwendung des Installationspakets eines Drittanbieter-Programms 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 vorher irgendwelche Installationspakete für Drittanbieter-Programme, die in der Kaspersky-Datenbank gelistet sind, erstellt haben, können Sie anschließend die Einstellungen dieser Pakete anzeigen und anpassen.

Das Anpassen der Einstellungen eines Installationspakets eines Drittanbieter-Programms steht nur unter der Lizenz für das Schwachstellen- und Patch-Management zur Verfügung.

Um die Einstelllungen eines Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank anzuzeigen und anzupassen:

1. Wechseln Sie im Hauptmenü zu **Gerätesuche und Bereitstellung → Bereitstellung und Zuweisung → Installationspakete**.
2. Klicken Sie in der Liste der Installationspakete auf den Namen des benötigten Installationspakets.

   Daraufhin wird das Eigenschaftenfenster geöffnet.
3. Ändern Sie bei Bedarf die Einstellungen.
4. Klicken Sie auf die Schaltfläche **Speichern**.

Die von Ihnen angepassten Einstellungen werden gespeichert.

Einstellungen eines Installationspakets eines Drittanbieter-Programms aus der Kaspersky-Datenbank

Die Einstellungen für das Installationspaket eines Drittanbieter-Programms sind auf den folgenden Registerkarten gruppiert:

Standardmäßig werden nicht alle der unten aufgeführten Einstellungen 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, welches den Namen des Installationspakets enthält und manuell angepasst werden kann
  - **Programm**

    Name des Drittanbieter-Programms, für welches das Installationspaket erstellt wurde.
  - **Version**

Versionsnummer des Drittanbieter-Programms, für welches das Installationspaket erstellt wurde.

- **Größe**

  Größe des Installationspakets (in Kilobyte).

- **Erstellt**

  Datum und Uhrzeit der Erstellung des Installationspakets.

- **Pfad**

  Pfad des Netzwerkordners, in dem sich das Installationspaket des Drittanbieter-Programms 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 anzeigt, und über folgende Spalten verfügt:

    - **Name**

      Der Name des Updates.

    - **Beschreibung**

      Die Beschreibung des Updates.

    - **Quelle**

      Die Quelle des Updates, d. h. entweder von Microsoft oder von einem anderen Dritthersteller veröffentlicht.

    - **Typ**

      Der Typ des Updates, d. h. entweder für einen Treiber oder für ein Programm vorgesehen.

    - **Kategorie**

Die für Microsoft-Updates angegebene Kategorie des Windows Server Update-Dienstes (WSUS) (Kritische Updates, Definitionsupdates, Treiber, Funktionspakete, Sicherheitsupdates, Servicepakete, 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**

  Die Ereigniskategorie eines Patches, wenn dieser für ein Kaspersky-Programm vorgesehen ist.

- **Artikel**

  Die ID des Artikels, welcher das Update beschreibt, in der Wissensdatenbank.

- **Bulletin**

  Die ID des Security-Bulletins, welches das Update beschreibt.

- **Nicht zur Installation bestimmt (neue Version)**

  Gibt an, ob das Update den Status "Nicht zur Installation zugewiesen" besitzt.

- **Bestimmt für die Installation**

  Gibt an, ob das Update den Status "Zur Installation" besitzt.

- **Wird installiert**

  Gibt an, ob das Update den Status "Installation" 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 Datum und Uhrzeit an, wann das Update registriert wurde.

- **Wird im interaktiven Modus installiert**

  Gibt an, ob das Update während der Installation Benutzerinterkation 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.

- **Programmversion**

  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 Herstellers des Updates an.

- **Programmfamilie**

  Gibt den Namen der Programmfamilie an, zu welcher dieses Update gehört.

- **Programm**

  Gibt den Namen des Programms an, zu welchem 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 zugewiesen (neue Version)" besitzt.

- Erforderliche Komponenten müssen installiert werden

  Gibt an, ob das Update den Status "Erfordert vorbereitende Installation" 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 anzeigt und über folgende Spalten verfügt:

  - **Revision** – Revisionsnummer des Installationspakets.
  - **Uhrzeit** – Datum und Uhrzeit der Änderung der 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 am Installationspaket während der Revision durchgeführt wurden.
  - **Beschreibung** – Beschreibung der Revision der am Installationspaket vorgenommenen Änderungen

    Standardmäßig ist die Beschreibung der Revision leer. 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.

Schließen von Schwachstellen in einem isolierten Netzwerk

In diesem Abschnitt werden die Schritte beschrieben, die Sie unternehmen können, um Schwachstellen in Programmen von Drittanbietern auf verwalteten Geräten zu schließen, 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 Programmen von Drittanbietern beheben, die auf den verwalteten Geräten in einem isolierten Netzwerk installiert sind. Solche Netzwerke umfassen sowohl Administrationsserver als auch die mit ihnen verbundenen verwalteten Geräte ohne Internetzugang. Um in so einer Art von Netzwerk Schwachstellen 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 Drittanbieter-Software-Updates herunterladen, aber keine Updates für Microsoft-Software auf isolierte Administrationsserver.

Weitere Informationen zum Prozess des Schließens von Schwachstellen in einem isolierten Netzwerk finden Sie in der Beschreibung und dem Schema dieses Prozesses.

Erforderliche Vorrausetzungen

Führen Sie vor dem Start Folgendes durch:

1. Weisen Sie ein Gerät für die Verbindung mit dem Internet und das Herunterladen von Patches zu. Dieses Gerät wird als Administrationsserver mit Internetzugang angesehen.
2. Installieren Sie Kaspersky Security Center Linux Version 15.1 oder höher auf den folgenden Geräten:
   - Zugewiesenes Gerät, welches als Administrationsserver mit Internetzugang fungiert
   - Isolierte Geräte, welche als Administrationsserver fungieren, die vom Internet isoliert sind (im Folgenden als isolierte Administrationsserver bezeichnet)
3. Stellen Sie sicher, dass jeder Administrationsserver über ausreichend Speicherplatz zum Herunterladen und Speichern der Updates und Patches verfügt.

Schritte

Das Installieren von Updates und das Schließend von Schwachstellen in Programmen von Drittanbietern auf den verwalteten Geräten isolierter Administrationsserver umfasst die folgenden Phasen:

1. **Konfiguration des Administrationsservers mit Internetzugang**

Bereiten Sie Ihren Administrationsserver mit Internetzugang vor, um Anfragen zu erforderlichen Software-Updates von Drittanbietern 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 verwenden, die vom Administrationsserver mit Internetzugang heruntergeladen wurden. Nach der Konfiguration versuchen die isolierten Administrationsserver nicht mehr, Patches aus dem Internet herunterzuladen. Stattdessen erhalten sie Updates mittels Patches.

3. **Übertragen von Patches und Installieren von Updates auf isolierten Administrationsservern**

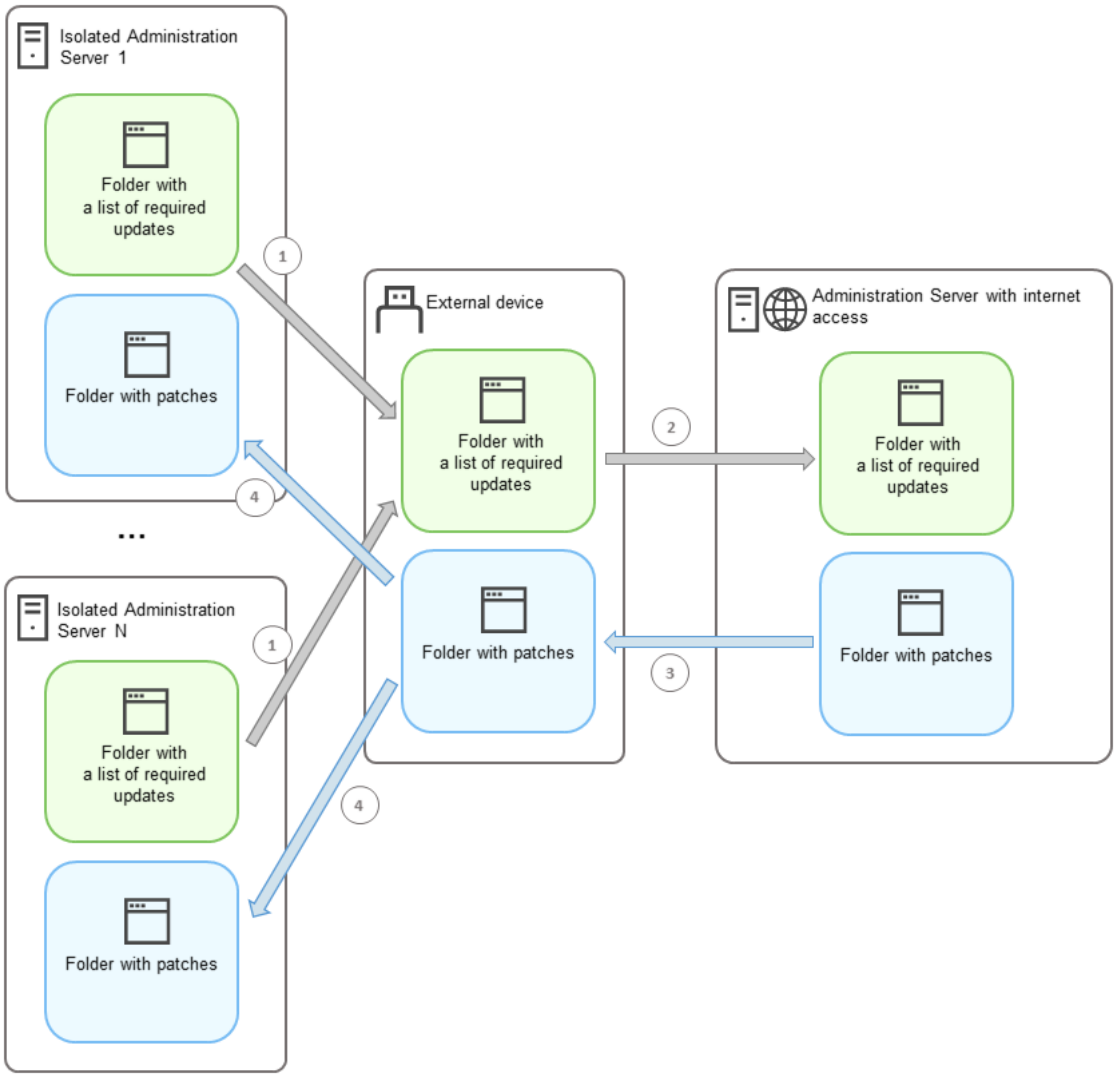
   Nachdem Sie die Konfiguration der Administrationsserver abgeschlossen haben, können Sie die Übertragung der Liste mit erforderlichen Updates und Patches vom Administrationsserver mit Internetzugang zu den isolierten Administrationsservern vornehmen. Anschließend werden unter Verwendung der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* die Updates der Patches auf den verwalteten Geräten installiert.

Ergebnisse

Als Ergebnis werden die Software-Updates von Drittanbietern 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 Updates beliebig oft erhalten, beispielsweise ein- oder mehrmals am Tag.

Über das Beheben von Schwachstellen in Programmen von Drittanbietern in einem isolierten Netzwerk

Der Prozess zum Beheben von Schwachstellen in Programmen von Drittanbietern in einem isolierten Netzwerk ist nachfolgend in der Abbildung beschrieben. Sie können diesen Vorgang regelmäßig wiederholen.



Der Prozess zur Übertragung der Patches und der Liste mit erforderlichen Updates zwischen dem Administrationsserver mit Internetzugang und den isolierten Administrationsservern

Jeder vom Internet isolierte Administrationsserver (im Folgenden als isolierter Administrationsserver bezeichnet) 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, die jeweils nach der ID des Patches benannt sind, der das erforderliche Update enthält. Daher entspricht jede Datei in der Liste einem bestimmten Patch.

Diese Liste der erforderlichen Updates wird über ein externes Gerät vom isolierten Administrationsserver an den angegebenen Administrationsserver mit Internetzugang übertragen. Anschließend lädt der festgelegte Administrationsserver die Patches aus dem Internet herunter und legt sie in einem angegebenen Ordner ab.

Nachdem alle Patches heruntergeladen und im angegebenen Ordner abgelegt wurden, werden sie auf alle isolierten Administrationsserver zurück 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* Patches aus und installiert 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 Übertragen von Patches innerhalb eines isolierten Netzwerks vorzubereiten, müssen Sie als Erstes 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:

   - Einen Ordner für die Liste mit erforderlichen Updates
   - Ordner für Patches

   Sie können diesen Ordnern einen beliebigen Namen geben.

2. Gewähren Sie in den erstellten Ordnern unter Verwendung der Standardverwaltungstools des Betriebssystems der Gruppe "KLAdmins" die Berechtigung zum **Ändern**.

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 die folgenden Befehle in der Befehlszeile aus:

   - So legen Sie den Pfad zum Patch-Ordner fest:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_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_IMPORT_PATH -t s -v "<Pfad zum Ordner>"`

   Beispiel: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -ts -v "/OrdnerFürPatches"`

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>`

   Standardmäßig ist der Wert auf 120 Sekunden eingestellt.

   Beispiel: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 120`

6. Starten Sie den Dienst des Administrationsservers 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 jeden isolierten Administrationsserver in Ihrem Netzwerk vor, damit Sie auf verwalteten Geräten, die mit isolierten Administrationsservern verbunden sind, Schwachstellen schließen und Updates installieren.

Um isolierte Administrationsserver zu konfigurieren, führen Sie die folgenden Schritte für jeden der Administrationsserver 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:
   - Einen Ordner für die Liste mit erforderlichen Updates
   - Ordner für Patches

   Sie können diesen Ordnern einen beliebigen Namen geben.
3. Gewähren Sie in den erstellten Ordnern unter Verwendung der Standardverwaltungstools des Betriebssystems der Gruppe "KLAdmins" die Berechtigung zum **Ändern**.
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 die folgenden Befehle in der Befehlszeile aus:
   - So legen Sie den Pfad zum Patch-Ordner fest:
     `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 "/OrdnerFuerPatches"`
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 können Sie sicherstellen, 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 deren Hashes und vergleicht die erfassten Werte mit den Hashes, die in der Datenbank des Administrationsservers gespeichert sind. Wenn der berechnete Hash nicht mit dem Hash in der Datenbank übereinstimmt, tritt ein Fehler auf und Sie müssen den inkorrekten Patch ersetzen.
8. Erstellen und Ausführen der Aufgabe *Suche nach Schwachstellen und erforderlichen Updates*. Starten Sie die Aufgabe manuell, wenn Sie möchten, dass sie früher ausgeführt wird, als im Aufgabenzeitplan angegeben.
9. Starten Sie den Dienst des Administrationsservers neu.

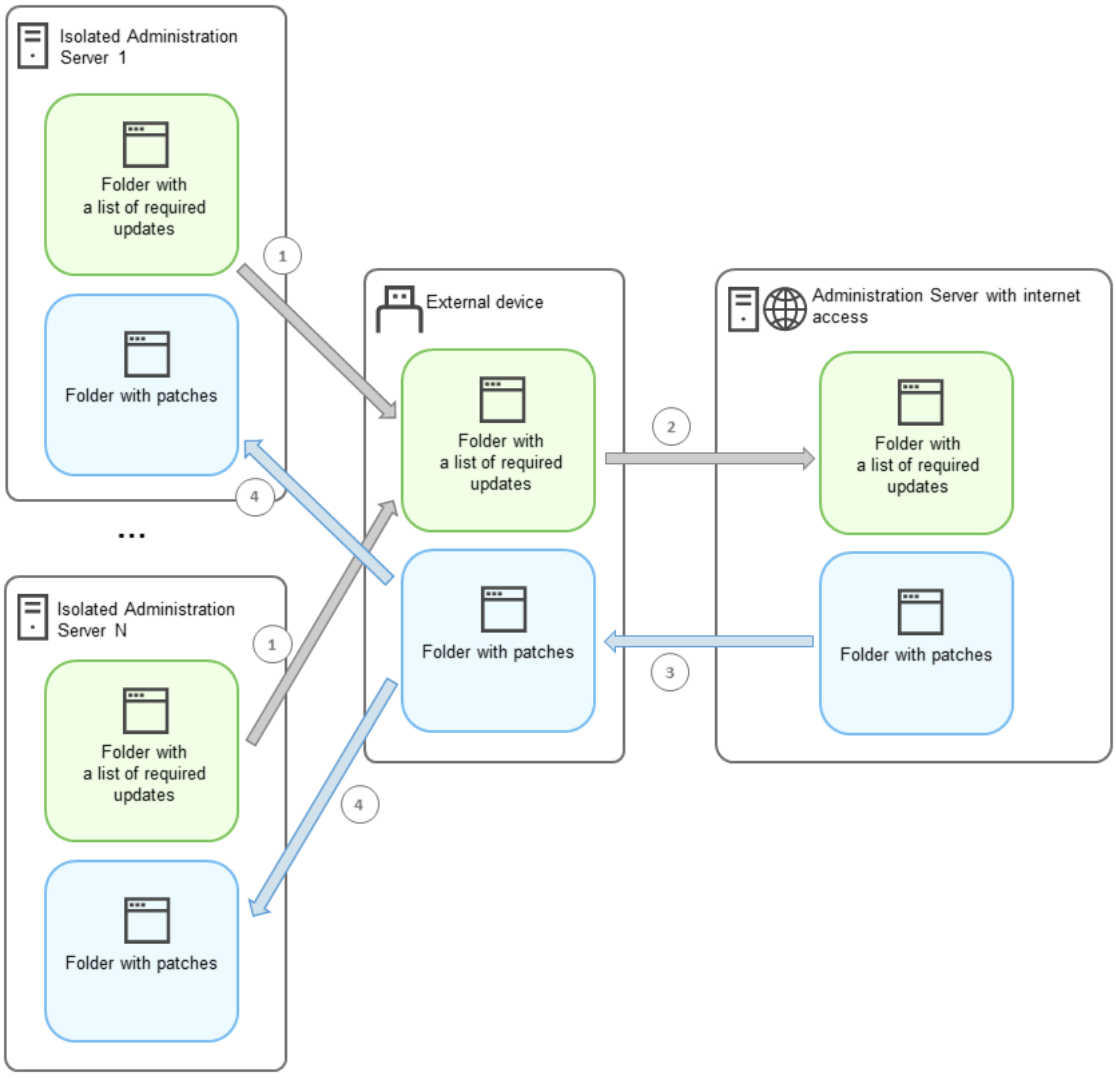
Nachdem Sie alle Administrationsserver konfiguriert haben, können Sie die Patches und die Liste mit erforderlichen Updates übertragen und Schwachstellen in Programmen von Drittanbietern auf den verwalteten Geräten innerhalb eines isolierten Netzwerks beheben.

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 Geräte, 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 Prozess zur Übertragung der Patches und der Liste mit erforderlichen Updates ist in der nachfolgenden Abbildung dargestellt:



Der Prozess zur Übertragung der 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 sie 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 einen beliebigen Namen geben.

   Wenn Sie diese Ordner bereits erstellt haben, löschen Sie diese.

4. Kopieren Sie die Liste der erforderlichen Updates von jedem isolierten Administrationsserver und fügen Sie diese Liste in den Ordner für die Liste mit erforderlichen Updates auf dem externen Gerät ein.

   Auf diese Weise vereinen Sie alle Listen, die von allen isolierten Administrationsservern erfasst wurden, in einem Ordner. 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 in den Ordner für die Liste mit erforderlichen Updates auf dem Administrationsserver mit Internetzugang ein.

   Auf dem Administrationsserver werden alle erforderlichen Patches automatisch aus dem Internet in den Ordner für Patches heruntergeladen. Dies kann mehrere Stunden dauern.

7. Stellen Sie sicher, dass alle erforderlichen Patches heruntergeladen wurden. Dies können Sie folgendermaßen tun:

   - Überprüfen Sie den Patch-Ordner 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.

   - Bereiten Sie ein spezielles Skript (z. B. ein Shell-Skript) vor. Wenn Sie eine große Anzahl von Patches erhalten, ist es schwierig, selbst zu überprüfen, ob alle Patches heruntergeladen wurden. In solchen Fällen ist es besser, die Prüfung zu automatisieren.

8. Kopieren Sie die Patches von dem Administrationsserver mit Internetzugang und fügen Sie diese 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 Liste von tatsächlichen 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 Administrationsserver gelangen, verarbeitet die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* diese Patches. Auf diese Weise werden Updates auf verwalteten Geräten installiert und Schwachstellen in Programmen von Drittanbietern behoben.

Wenn die Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* ausgeführt wird, starten Sie das Gerät des Administrationsservers nicht neu und führen Sie nicht die Aufgabe *Backup der Daten des Administrationsservers anlegen* aus (sie führt ebenfalls zu einem Neustart). Dies führt zur Unterbrechung der Aufgabe *Erforderliche Updates installieren und Schwachstellen schließen* und die Updates werden nicht installiert. In diesem Fall müssen Sie diese Aufgabe manuell neu starten oder warten, bis die Aufgabe gemäß dem konfigurierten Zeitplan gestartet wird.

Übertragen von Patches und Installieren von Updates in einem isolierten Netzwerk deaktivieren

Sie können die Übertragung von Patches an isolierten Administrationsservern deaktivieren. Dies kann nützlich sein, wenn Sie einen oder mehrere Administrationsserver aus dem isolierten Netzwerk herausnehmen möchten. Sie können dadurch die Anzahl der Patches und die Zeit für deren Download 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 in dem 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 die folgenden Befehle in der Befehlszeile aus:

   - So löschen Sie den Pfad des Ordners mit den 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 zu den Ordnern für die Patches und für die Liste der erforderlichen Updates.

   Führen Sie die folgenden Befehle in der Befehlszeile unter einem Benutzerkonto mit Root-Rechten aus:

   - So löschen Sie den Pfad des Ordners mit den Patches:
     ```
     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 von jedem Administrationsserver neu, auf dem Sie die Pfade zu den Ordnern gelöscht haben.

Wenn Sie den Administrationsserver mit Internetzugang neu konfiguriert haben, werden keine Patches mehr über Kaspersky Security Center Linux 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 zukünftig die Behebung von Schwachstellen auf deaktivierten isolierten Administrationsservern aktivieren möchten, müssen Sie diese Administrationsserver und den Administrationsserver mit Internetzugang erneut 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:

1. Laden Sie das Archiv KlAkOAPI.tar.gz herunter. Dieses Archiv enthält das KlAkOAPI-Paket sowie Beispiele (Sie können diese aus dem Archiv oder dem OpenAPI-Referenzhandbuch kopieren). Das Archiv "KlAkOAPI.tar.gz" befindet sich ebenfalls im Installationsordner von Kaspersky Security Center Linux.

2. Installieren Sie das Paket KlAkOAPI aus dem Archiv KlAkOAPI.tar.gz auf einem Gerät mit installiertem Administrationsserver.

   Sie können nur auf Geräten, auf denen der Administrationsserver und das Paket KlAkOAPI installiert sind, OpenAPI-Methoden aufrufen, Beispiele ausführen und eigene Skripte ausführen.

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
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 Programme
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 Programme 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	Aufgaben verwalten

	Sie können auch eine Aufgabe starten. Standardmäßig startet das Beispiel eine Aufgabe, nachdem es Statistiken ausgegeben hat.	
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.	Erstellen einer Aufgabe
Lizenzschlüssel durchzählen	Sie können eine Liste mit allen aktiven Lizenzschlüsseln für Kaspersky-Programme 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
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

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.

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
- 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.

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.

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

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	24 GB
Speicherplatz	250 GB, 150 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	8 Kerne, 2500 MHz
Arbeitsspeicher	18 GB
Speicherplatz	200 GB, 150 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 davon abgeraten, die Größe des Transportprotokolls explizit einzuschränken (standardmäßig die Datei KAV_log.LDF, falls das DBMS "SQL Server" verwendet wird). Behalten Sie den Standardwert des Parameters MAXSIZE bei. Wenn Sie jedoch die Größe dieser Datei begrenzen müssen, berücksichtigen Sie dabei, dass der üblicherweise erforderliche Wert des Parameters MAXSIZE für KAV_log.LDF 20480 MB beträgt.

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 Datenbank des Administrationsservers 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 Datenbank des Administrationsservers 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.

Voraussetzungen für Verteilungspunkte

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.

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	Anzahl der Verteilungspunkte

Netzwerksegment	
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 Datenbank des Administrationsservers 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).

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 Verschieben von Daten ins Backup, 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
- Pflege von Datenbanken

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.

Aufgabe zur Inventarisierung von Software

Sie können die Auslastung der Datenbank verringern und gleichzeitig Informationen über die installierten Anwendungen erhalten. Dazu empfehlen wir, dass Sie eine Bestandsaufnahme 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
Gemeinsame 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
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 des Programms nicht kritisch sind:

- Die Richtlinie von Kaspersky Endpoint Security für Windows zeigt eine Schutzstufe an, die nicht der Schutzstufe entspricht, die in Kaspersky Endpoint Security für Windows angezeigt wird.

- Wenn Sie in einer dreistufigen Serverhierarchie den Server der dritten Ebene öffnen und dessen primären Server von einem Server der zweiten Ebene in einen Server der ersten Ebene ändern, zeigt Kaspersky Security Center Linux weiterhin die entfernte hierarchische Verbindung zwischen den Servern der zweiten und dritten Ebene an.

- 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.

- Kaspersky Security Center Linux kann auf einem Gerät mit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.8) nicht installiert werden, wenn der Modus für geschlossene Software-Umgebungen deaktiviert ist.

- Kaspersky Security Center Linux wird auf einem Gerät mit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.8) nicht gestartet, wenn Sie nach der Installation von Kaspersky Security Center Linux den Modus für eine geschlossene Software-Umgebung aktivieren.

- Die Kaspersky Security Center Web Console startet nach der Installation auf einem Gerät mit Astra Linux Special Edition RUSB.10015-01 (operatives update 1.7) nicht, wenn das Betriebssystem in der geschlossenen Softwareumgebung ausgeführt wird.

- Kaspersky Security Center Linux kann auf einem Gerät mit Astra Linux Special Edition RUSB.10015-01 (operatives Update 1.7) nicht installiert werden, wenn das Betriebssystem in der geschlossenen Softwareumgebung ausgeführt wird.

- Der Administrationsagent wird auf einem verwalteten Gerät mit CentOS 6.6 nicht neu gestartet, nachdem sein Prozess durch ein Kill-Befehl beendet wurde.

- Wenn Sie die Aufgabe *Kennwort des Benutzerkontos ändern (nur Linux)* für einen Benutzer erstellen und die Option **Dies ist ein Einmalkennwort (der Benutzer muss das Kennwort nach dem ersten Anmelden ändern)** aktivieren, kann sich der Benutzer nach dem Ändern des Einmalkennworts nicht in Kaspersky Security Center Web Console anmelden.

- Sie können Kaspersky Endpoint Security for Linux auf einem verwalteten Gerät nicht über das Tools zur Remote-Dignose starten oder stoppen.

- 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.

- Kaspersky Endpoint Security für Windows unterstützt den KSN Proxy-Dienst nicht, wenn in den Eigenschaften des Administrationsservers für die KSN Proxy-Einstellungen die Option **HTTPS verwenden** aktiviert ist und die Adresse des Administrationsservers nicht-lateinische Symbole enthält.

- Die in der Richtlinie für Kaspersky Endpoint Security für Windows angezeigte Schutzstufe entspricht nicht der Schutzstufe in der Benutzeroberfläche von Kaspersky Endpoint Security für Windows.

- Wenn ein Programm aus dem Abschnitt **Programm-Registry** auf einem Linux-Gerät gefunden wurde, enthalten die Programmeigenschaften keine Informationen über zugehörige ausführbare Dateien.

- Bei Berichten im Letter-Format kann ein Seitenumbruch eine Textzeile horizontal unterbrechen.

- Wenn Sie im Assistenten **Sekundären Administrationsserver hinzufügen** ein Konto mit aktivierter zweistufiger Überprüfung auf dem zukünftigen sekundären Server angeben, wird der Assistent mit einem Fehler beendet. Um dieses Problem zu beheben, geben Sie ein Konto an, für das die zweistufige Überprüfung deaktiviert ist, oder erstellen Sie die Hierarchie vom zukünftigen sekundären Server.

- 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.

- 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.

- Sobald die Aufgabe *Skripte remote ausführen* gestartet wurde, können Sie das ihr zugewiesene Benutzerkonto nicht mehr ändern. Um das der Aufgabe zugewiesene Benutzerkonto zu ändern, beenden Sie die Aufgabe in den Aufgabeneinstellungen und starten Sie diese anschließend mit den korrekten Einstellungen erneut.

- Die Aufgabe *Kennwort des Benutzerkontos ändern* funktioniert möglicherweise nicht korrekt, wenn SELinux auf dem Benutzergerät aktiviert ist. Weitere Informationen zum Deaktivieren von SELinux finden Sie in der entsprechenden Dokumentation für Ihr Betriebssystem.

Anfragen an den Technischen Support

Dieser Abschnitt beschreibt, wie Sie technischen Support erhalten können, und nennt die dafür notwendigen Voraussetzungen.

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 Webseite des Produkt-Supports mit dem Produktlebenszyklus). 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 Seite des Technischen Supports
- Versand einer Anfrage an den Technischen Support aus dem 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 Kontaktaufnahme mit den Spezialisten von Kaspersky über elektronische Anfragen. Sie können Kaspersky CompanyAccount verwenden, um den Status Ihrer Online-Anfragen zu verfolgen sowie deren Verlauf zu speichern.

Sie können alle Mitarbeiter Ihrer Firma unter einem Benutzerkonto für Kaspersky CompanyAccount registrieren. Mithilfe eines einheitlichen Benutzerkontos 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 Website 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 werden so lange gespeichert, wie sich Kaspersky Security Center Linux in Verwendung befindet. Wenn Kaspersky Security Center Linux entfernt wird, werden auch die Dump-Dateien endgültig gelöscht. Die 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 zum Programm

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 des Programms.

Neben Fragen zu Kaspersky Security Center Linux können die Artikel auch andere Programme von Kaspersky betreffen. Artikel in der Wissensdatenbank können auch Neuigkeiten über den Technischen Support enthalten.

In der Community über Anwendungen von Kaspersky 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 Programmen von Kaspersky ermöglicht wird, die auf einem bestimmten Netzwerk-Knoten (Workstation oder Server) installiert sind. Diese Komponente ist für alle von dem Unternehmen entwickelten Programme für Microsoft® Windows® einheitlich. Für Programme von Kaspersky, 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 Programmen von Kaspersky gruppiert sind. Geräte sind zur erleichterten Verwaltung als einzelne Entität gruppiert. Eine Gruppe kann andere Gruppen beinhalten. Für jedes installierte Programm in der Gruppe können Gruppenrichtlinien und Gruppenaufgaben erstellt werden.

Administrationsserver

Eine Komponente von Kaspersky Security Center Linux, die Informationen über alle Programme von Kaspersky, die innerhalb des Unternehmensnetzwerks installiert sind, zentral speichert. Sie kann auch zur Verwaltung dieser Programme verwendet werden.

Administrationsserver-Client (Client-Gerät)

Gerät, Server oder Workstation, auf welchem bzw. welcher der Administrationsagent installiert ist und verwaltete Programme von Kaspersky 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 Programmvorgänge über das zentralisierte Remote-Verwaltungssystem Kaspersky Security Center Linux 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 Programmen von Kaspersky.

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 vom Programm 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 ein Programm von Kaspersky 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

Programmeinstellungen, 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. Typische Cloud-Dienste sind beispielsweise Microsoft Teams, Salesforce und Microsoft Office 365. Die Cloud-Dienste werden in Kategorien wie *Datenaustausch*, *Messenger* oder *E-Mail* eingeteilt.

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 Programmverwaltung

Programmverwaltung über eine lokale Schnittstelle.

Ereignis-Datenverwaltung

Ein Teil der Datenbank des Administrationsservers. 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 des Programms 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.

Inkompatibles Programm

Ein Antiviren-Programm eines Drittanbieters oder ein Kaspersky-Programm, das die Verwaltung über Kaspersky Security Center Linux nicht unterstützt.

Installationspaket

Satz von Dateien, der für die Remote-Installation eines Kaspersky-Programms 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.

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 Programme von Kaspersky 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.

Lizenzierte Programmgruppe

Gruppe von Programmen, die auf der Grundlage von Kriterien erstellt wird, die vom Administrator festgelegt werden (beispielsweise nach Hersteller), für die Statistiken zu den Installationen auf Client-Geräten geführt werden.

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 einen manuellen Start der Installation aus dem Programmpaket des Programms zur Gewährleistung der Sicherheit oder 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.

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

Programmeinstellungen, die für alle Aufgabentypen gleich sind und den Gesamtbetrieb des Programms regeln, zum Beispiel Leistungseinstellungen, Berichtseinstellungen und Backup-Einstellungen.

Provisioning-Profil

Zusammenstellung von Einstellungen für die Ausführung von Programmen auf mobilen iOS-Geräten. Ein Provisioning-Profil enthält Informationen zur Lizenz und ist mit einer bestimmten App verbunden.

Remote-Installation

Installation von Kaspersky-Apps über die von Kaspersky Security Center Linux bereitgestellten Dienste.

Richtlinie

Eine Richtlinie bestimmt die Einstellungen eines Programms und verwaltet die Möglichkeit, dieses Programm auf Computern innerhalb einer Administrationsgruppe zu konfigurieren. Für jedes Programm muss eine eigene Richtlinie erstellt werden. Sie können mehrere Richtlinien für Programme, die auf Computern in mehreren Administrationsgruppen installiert sind, erstellen, es kann jedoch innerhalb einer Administrationsgruppe immer nur eine Richtlinie auf ein Programm 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, ein Programm von Kaspersky 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 eines Programms von Kaspersky 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 Programm-Module), 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 Programm-Module von Kaspersky einschließlich kritischer Updates, die sich über einen bestimmten Zeitraum angesammelt haben, und Änderungen an der Programmarchitektur.

Verschieben der Daten des Administrationsservers ins Backup

Kopieren der Daten des Administrationsservers als Backup und zur anschließenden Wiederherstellung mithilfe des Backup-Tools. Das Tool kann Folgendes speichern:

- 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 Programmen (Inhalt der Ordner Pakete, Update-Deinstallation)
- Zertifikat des Administrationsservers

Verteilungspunkt

Computer, auf dem der Administrationsagent installiert ist und der zur Update-Verteilung, zur Remote-Installation von Programmen 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 Backup 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-Computern
- Datenverwaltung der Installationsdateien zur Remote-Installation von Programmen (Inhalt der Ordner Pakete, Update-Deinstallation)
- Zertifikat des Administrationsservers

Zentralisierte Programmverwaltung

Remote-Programmverwaltung 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 Abonnementschlüssel

Ein Schlüssel, der das Recht auf Nutzung des Programms bestätigt, jedoch im Augenblick nicht aktiviert ist.

Informationen über den Code von Drittherstellern

Informationen über den Code von Drittherstellern finden Sie in der Datei legal_notices.txt, die sich im Installationsverzeichnis des Programms befindet.

Markenrechtliche Hinweise

Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer Besitzer.

Adobe, Acrobat, Flash, Shockwave und PostScript sind in den USA und/oder anderen Ländern eingetragene Markenzeichen oder Markenzeichen von Adobe.

AMD, AMD64 sind Warenzeichen oder eingetragene Marken 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.

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 Markenzeichen von Citrix Systems, Inc. und/oder einem oder mehreren seiner Tochtergesellschaften, und können im United States Patent and Trademark Office und in anderen Ländern eingetragen sein.

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 in den USA und/oder anderen Ländern.

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.

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.

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.

VMware, VMware vSphere und VMware Workstation sind eingetragene Markenzeichen oder Markenzeichen von VMware, Inc. in den USA und/oder anderen Ländern.

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.