kaspersky

Guida di Kaspersky Security Center 15 Linux

© 2025 AO Kaspersky Lab

Sommario

Guida di Kaspersky Security Center Linux

Novità

Informazioni su Kaspersky Security Center Linux

- Requisiti hardware e software
  - Requisiti di Administration Server
  - Requisiti di Web Console
  - Requisiti di Network Agent
- Kit di distribuzione
- Informazioni sulla compatibilità di Administration Server e Kaspersky Security Center Web Console
- Confronto tra Kaspersky Security Center basato su Windows e basato su Linux
- Informazioni di Kaspersky Security Center Cloud Console

Architettura e concetti di base

- Architettura
- Diagramma di distribuzione di Kaspersky Security Center Linux Administration Server e Kaspersky Security Center Web Console
- Porte utilizzate da Kaspersky Security Center Linux
- Porte utilizzate da Kaspersky Security Center Web Console
- Concetti di base
  - Administration Server
  - Gerarchia di Administration Server
  - Administration Server virtuale
  - Server Web
  - Network Agent
  - Gruppi di amministrazione
  - Dispositivo gestito
  - Dispositivo non assegnato
  - Workstation dell'amministratore
  - Plug-in Web di gestione
  - Criteri
  - Profili criterio
  - Attività
  - Ambito attività
  - Relazioni tra impostazioni locali delle applicazioni e criteri
  - Punto di distribuzione
  - Gateway di connessione

Schemi per traffico dati e utilizzo delle porte

- Administration Server e dispositivi gestiti nella LAN
- Administration Server primario nella LAN e due Administration Server secondari
- Administration Server nella LAN, dispositivi gestiti in Internet, proxy inverso in uso
- Administration Server nella LAN, dispositivi gestiti in Internet, gateway di connessione in uso
- Administration Server all'interno della rete perimetrale, dispositivi gestiti in Internet
- Interazione dei componenti di Kaspersky Security Center Linux e delle applicazioni di protezione: ulteriori informazioni
  - Convenzioni utilizzate negli schemi di interazione
  - Administration Server e DBMS
  - Administration Server e dispositivo client: gestione dell'applicazione di protezione
  - Upgrade del software in un dispositivo client tramite un punto di distribuzione

Gerarchia di Administration Server: Administration Server primario e Administration Server secondario
Gerarchia di Administration server con un Administration Server secondario nella rete perimetrale
Administration Server, un gateway di connessione in un segmento di rete e un dispositivo client
Administration Server e due dispositivi nella rete perimetrale: un gateway di connessione e un dispositivo client
Administration Server e Kaspersky Security Center Web Console
Operazioni preliminari
Installazione
Configurazione del server MariaDB x64 per l'utilizzo con Kaspersky Security Center Linux
Configurazione del server PostgreSQL o Postgres per l'utilizzo con Kaspersky Security Center Linux
Installazione di Kaspersky Security Center Linux
Installazione di Kaspersky Security Center Linux in modalità automatica
Installazione di Kaspersky Security Center Linux su Astra Linux in modalità ambiente software chiuso
Installazione di Kaspersky Security Center Web Console
Parametri di installazione di Kaspersky Security Center Web Console
Installazione di Kaspersky Security Center Web Console su Astra Linux in modalità ambiente software chiuso
Installazione di Kaspersky Security Center Web Console connesso all'Administration Server installato nei nodi del cluster di failover Kaspersky Security Center Linux
Distribuzione del cluster di failover Kaspersky Security Center Linux
Scenario: Distribuzione di un cluster di failover Kaspersky Security Center Linux
Informazioni sul cluster di failover Kaspersky Security Center Linux
Preparazione di un file server per un cluster di failover Kaspersky Security Center Linux
Preparazione dei nodi per un cluster di failover Kaspersky Security Center Linux
Installazione di Kaspersky Security Center Linux nei nodi del cluster di failover Kaspersky Security Center Linux
Avvio e arresto manuale dei nodi del cluster
Account per l'utilizzo del DBMS
Configurazione dell'account DBMS per l'utilizzo di MySQL e MariaDB
Configurazione dell'account DBMS per l'utilizzo di PostgreSQL e Postgres Pro
Certificati per l'utilizzo di Kaspersky Security Center Linux
Informazioni sui certificati di Kaspersky Security Center
Requisiti per i certificati personalizzati utilizzati in Kaspersky Security Center Linux
Riemissione del certificato per Kaspersky Security Center Web Console
Sostituzione del certificato per Kaspersky Security Center Web Console
Conversione di un certificato PFX nel formato PEM
Scenario: Specificazione del certificato di Administration Server personalizzato
Sostituzione del certificato di Administration Server con l'utilità klsetsrvcert
Connessione dei Network Agent ad Administration Server con l'utilità klmover
Definizione di una cartella condivisa
Accesso a Kaspersky Security Center Web Console e disconnessione
Modifica della lingua dell'interfaccia di Kaspersky Security Center Web Console
Configurazione del server MySQL x64 per l'utilizzo con Kaspersky Security Center Linux
Avvio rapido guidato
Passaggio 1. Definizione delle impostazioni della connessione Internet
Passaggio 2. Download degli aggiornamenti necessari
Passaggio 3. Selezione delle risorse da proteggere
Passaggio 4. Selezione del criptaggio nelle soluzioni
Passaggio 5. Configurazione dell'installazione dei plug-in per le applicazioni gestite
Passaggio 6. Download dei pacchetti di distribuzione e creazione dei pacchetti di installazione
Passaggio 7. Configurazione di Kaspersky Security Network

Passaggio 8. Selezione del metodo di attivazione dell'applicazione
Passaggio 9. Creazione di una configurazione della protezione di rete di base
Passaggio 10. Configurazione delle notifiche e-mail
Passaggio 11. Chiusura dell'Avvio rapido guidato
Distribuzione guidata della protezione
Passaggio 1. Avvio della Distribuzione guidata della protezione
Passaggio 2. Selezione del pacchetto di installazione
Passaggio 3. Selezione di un metodo per la distribuzione del file chiave o del codice di attivazione
Passaggio 4. Selezione della versione di Network Agent
Passaggio 5. Selezione dei dispositivi
Passaggio 6. Specificazione delle impostazioni dell'attività di installazione remota
Passaggio 7. Rimozione delle applicazioni incompatibili prima dell'installazione
Passaggio 8. Spostamento dei dispositivi in Dispositivi gestiti
Passaggio 9. Selezione degli account per l'accesso ai dispositivi
Passaggio 10. Avvio dell'installazione
Upgrade di Kaspersky Security Center Linux
Upgrade di Kaspersky Security Center Linux utilizzando il file di installazione
Upgrade di Kaspersky Security Center Linux tramite backup
Aggiornamento di Kaspersky Security Center Linux nei nodi del cluster di failover Kaspersky Security Center Linux
Upgrade di Kaspersky Security Center Web Console
Upgrade di Kaspersky Security Center Web Console su Astra Linux in modalità ambiente software chiuso
Migrazione a Kaspersky Security Center Linux
Esportazione di oggetti di gruppo da Kaspersky Security Center Windows
Importazione del file di esportazione in Kaspersky Security Center Linux
Passaggio dei dispositivi gestiti alla gestione di Kaspersky Security Center Linux
Configurazione di Administration Server
Configurazione della connessione di Kaspersky Security Center Web Console ad Administration Server
Configurazione di una lista di indirizzi IP consentiti per connettersi a Kaspersky Security Center Linux
Configurazione delle impostazioni di accesso a Internet per Administration Server
Gerarchia di Administration Server
Creazione di una gerarchia di Administration Server: l'aggiunta un Administration Server secondario
Visualizzazione dell'elenco degli Administration Server secondari
Gestione di Administration Server virtuali
Creazione di un Administration Server virtuale
Abilitazione e disabilitazione di un Administration Server virtuale
Assegnazione di un amministratore per un Administration Server virtuale
Modifica di Administration Server per i dispositivi client
Eliminazione di un Administration Server virtuale
Configurazione della registrazione degli eventi di connessione ad Administration Server
Impostazione del numero massimo di eventi nell'archivio eventi
Spostamento di Administration Server in un altro dispositivo
Modifica delle credenziali del DBMS
Backup e ripristino dei dati di Administration Server
Creazione di un'attività di backup dei dati di Administration Server
Utilizzo dell'utilità klbackup per eseguire il backup e il ripristino dei dati
Manutenzione di Administration Server
Eliminazione di una gerarchia di Administration Server
Accesso ai server DNS pubblici

- Configurazione dell'interfaccia
- Criptaggio delle comunicazioni con TLS
- Elenco globale delle subnet

Individuazione dei dispositivi nella rete
- Scenario: Individuazione dei dispositivi nella rete
- Polling intervallo IP
- Aggiunta e modifica di un intervallo IP
- Polling zeroconf
- Polling del controller di dominio
- Autenticazione e connessione a un controller di dominio
- Configurazione di un controller di dominio Samba
- Utilizzo della modalità dinamica VDI nei dispositivi client
  - Abilitazione della modalità dinamica VDI nelle proprietà di un pacchetto di installazione per Network Agent
  - Spostamento dei dispositivi da VDI a un gruppo di amministrazione

Best practice per la distribuzione
- Guida all'hardening
  - Distribuzione di Administration Server
  - Sicurezza della connessione
  - Account e autenticazione
  - Gestione della protezione di Administration Server
  - Gestione della protezione dei dispositivi client
  - Configurazione della protezione per le applicazioni gestite
  - Manutenzione di Administration Server
  - Trasferimento di eventi a sistemi di terzi
  - Scenario: autenticazione di MySQL Server
  - Scenario: autenticazione del server PostgreSQL
- Preparazione per la distribuzione
  - Pianificazione della distribuzione di Kaspersky Security Center Linux
    - Schemi tipici di distribuzione di un sistema di protezione
    - Informazioni sulla pianificazione della distribuzione di Kaspersky Security Center Linux nella rete di un'organizzazione
    - Selezione di una struttura per la protezione di un'azienda
    - Configurazioni standard di Kaspersky Security Center Linux
      - Configurazione standard: singola sede
      - Configurazione standard: poche sedi su larga scala gestite da amministratori distinti
      - Configurazione standard: più sedi remote di piccole dimensioni
    - Selezione di un DBMS
    - Concessione dell'accesso via Internet all'Administration Server
      - Accesso a Internet: Administration Server in una rete locale
      - Accesso a Internet: Administration Server in una rete perimetrale
    - Informazioni sui punti di distribuzione
    - Aumento del limite dei descrittori di file per il servizio klnagent
    - Calcolo del numero e configurazione dei punti di distribuzione
    - Administration Server virtuali
  - Impostazioni di rete per l'interazione con servizi esterni
- Distribuzione di Network Agent e dell'applicazione di protezione
  - Distribuzione iniziale
    - Configurazione dei programmi di installazione
    - Pacchetti di installazione

Informazioni sulle attività di installazione remota in Kaspersky Security Center Linux
Distribuzione tramite l'acquisizione e la copia dell'immagine di un dispositivo
Modalità di clonazione del disco di Network Agent
Distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center Linux
Esecuzione di pacchetti indipendenti creati tramite Kaspersky Security Center Linux
Installazione remota delle applicazioni nei dispositivi in cui è installato Network Agent
Gestione dei riavvii dei dispositivi nell'attività di installazione remota
Aggiornamento dei database in un pacchetto di installazione di un'applicazione di protezione
Monitoraggio della distribuzione
Configurazione dei programmi di installazione
Informazioni generali
Parametri di installazione di Administration Server
Parametri di installazione di Network Agent
Infrastruttura virtuale
Suggerimenti per la riduzione del carico sulle macchine virtuali
Supporto delle macchine virtuali dinamiche
Supporto della copia delle macchine virtuali
Supporto del rollback del file system per i dispositivi con Network Agent
Installazione locale delle applicazioni
Installazione di Network Agent per Linux in modalità interattiva
Installazione di Network Agent per Windows in modalità interattiva
Installazione di Network Agent for Windows in modalità automatica
Installazione di applicazioni in modalità automatica
Installazione delle applicazioni tramite pacchetti indipendenti
Impostazioni del pacchetto di installazione di Network Agent
Configurazione manuale dell'attività di gruppo per la scansione di un dispositivo con Kaspersky Endpoint Security
Gestione dei dispositivi client
Impostazioni di un dispositivo gestito
Regole di spostamento dei dispositivi
Creazione delle regole di spostamento dei dispositivi
Copia delle regole di spostamento dei dispositivi
Condizioni di una regola di spostamento dei dispositivi
Aggiunta manuale dei dispositivi a un gruppo di amministrazione
Spostamento manuale dei dispositivi o dei cluster in un gruppo di amministrazione
Informazioni sui cluster e sugli array di server
Proprietà di un cluster o di un array di server
Regolazione di punti di distribuzione e gateway di connessione
Configurazione standard dei punti di distribuzione: singola sede
Configurazione standard dei punti di distribuzione: più sedi remote di piccole dimensioni
Calcolo del numero e configurazione dei punti di distribuzione
Assegnazione automatica di punti di distribuzione
Assegnazione manuale di punti di distribuzione
Modifica dell'elenco dei punti di distribuzione per un gruppo di amministrazione
Abilitazione di un server push
Informazioni sugli stati dei dispositivi
Configurazione del passaggio degli stati del dispositivo
Selezioni dispositivi
Visualizzazione dell'elenco dei dispositivi da una selezione di dispositivi

Creazione di una selezione dispositivi
Configurazione di una selezione dispositivi
Esportazione dell'elenco dei dispositivi da una selezione di dispositivi
Rimozione di dispositivi dai gruppi di amministrazione in una selezione
Tag dispositivo
Creazione di un tag dispositivo
Ridenominazione di un tag dispositivo
Eliminazione di un tag dispositivo
Visualizzazione dei dispositivi a cui è assegnato un tag
Visualizzazione dei tag assegnati a un dispositivo
Tagging manuale di un dispositivo
Rimozione di un tag assegnato a un dispositivo
Visualizzazione delle regole per il tagging automatico dei dispositivi
Modifica di una regola per il tagging automatico dei dispositivi
Creazione di una regola per il tagging automatico dei dispositivi
Esecuzione di regole per il tagging automatico dei dispositivi
Eliminazione di una regola per il tagging automatico dei dispositivi
Gestione dei tag del dispositivo tramite l'utilità klscflag
Criptaggio e protezione dei dati
Visualizzazione dell'elenco delle unità criptate
Visualizzazione dell'elenco degli eventi di criptaggio
Creazione e visualizzazione di rapporti sul criptaggio
Concedere l'accesso a un'unità criptata in modalità offline
Modifica di Administration Server per i dispositivi client
Spostamento dei dispositivi connessi ad Administration Server tramite gateway di connessione a un altro Administration Server
Visualizzazione e configurazione delle azioni per i dispositivi inattivi
Invio di messaggi agli utenti dei dispositivi
Accensione, spegnimento e riavvio dei dispositivi client in remoto
Gestione dei gruppi di amministrazione
Creazione dei gruppi di amministrazione
Installazione automatica delle applicazioni nei dispositivi di un gruppo di amministrazione
Spostamento di gruppi di amministrazione
Eliminazione di gruppi di amministrazione
Distribuzione delle applicazioni Kaspersky
Scenario: Distribuzione delle applicazioni Kaspersky
Aggiunta dei plug-in di gestione per le applicazioni Kaspersky
Download e creazione dei pacchetti di installazione per le applicazioni Kaspersky
Creazione di pacchetti di installazione da un file
Creazione di pacchetti di installazione indipendenti
Modifica del limite relativo alle dimensioni dei dati del pacchetto di installazione personalizzato
Installazione di Network Agent per Linux in modalità automatica (con un file di risposte)
Preparazione di un dispositivo in cui viene eseguito Astra Linux in modalità ambiente software chiuso per l'installazione di Network Agent
Visualizzazione dell'elenco dei pacchetti di installazione indipendenti
Distribuzione dei pacchetti di installazione agli Administration Server secondari
Preparazione di un dispositivo Linux e installazione di Network Agent in un dispositivo Linux da remoto
Installazione delle applicazioni tramite un'attività di installazione remota
Installazione remota di un'applicazione

Installazione di applicazioni negli Administration Server secondari
Definizione delle impostazioni per l'installazione remota nei dispositivi Unix
Avvio e arresto delle applicazioni Kaspersky.
Sostituzione di applicazioni di protezione di terzi
Rimozione di applicazioni o aggiornamenti software in remoto
Preparazione di un dispositivo che esegue SUSE Linux Enterprise Server 15 per l'installazione di Network Agent
Preparazione di un dispositivo Windows per l'installazione remota
Preparazione di un dispositivo macOS per l'installazione remota di Network Agent
Licensing
Licensing di Kaspersky Security Center Linux.
Informazioni sul Contratto di licenza con l'utente finale
Informazioni sulla licenza
Informazioni sul certificato di licenza
Informazioni sulla chiave di licenza
Visualizzazione dell'Informativa sulla privacy
Opzioni di licensing per Kaspersky Security Center
Informazioni sul file chiave
Informazioni sulla trasmissione dei dati
Informazioni sull'abbonamento
Attivazione di Kaspersky Security Center Linux
Licensing delle applicazioni Kaspersky gestite
Licensing delle applicazioni gestite
Aggiunta di una chiave di licenza all'archivio dell'Administration Server
Distribuzione di una chiave di licenza ai dispositivi client
Distribuzione automatica di una chiave di licenza
Visualizzazione delle informazioni sulle chiavi di licenza in uso
Eventi di superamento del limite di licenze
Eliminazione di una chiave di licenza dall'archivio
Revoca del consenso a un Contratto di licenza con l'utente finale
Rinnovo delle licenze per le applicazioni Kaspersky
Utilizzo di Kaspersky Marketplace per scegliere le soluzioni aziendali Kaspersky
Configurazione delle applicazioni Kaspersky
Scenario: Configurazione della protezione di rete
Informazioni sui metodi di gestione della protezione incentrati sui dispositivi e incentrati sugli utenti
Configurazione e propagazione dei criteri: approccio incentrato sui dispositivi
Configurazione e propagazione dei criteri: approccio incentrato sull'utente
Criteri e profili criterio
Informazioni su criteri e profili criterio
Informazioni su blocco e impostazioni bloccate
Ereditarietà di criteri e profili criterio
Gerarchia dei criteri
Profili criterio in una gerarchia di criteri
Modalità di implementazione delle impostazioni in un dispositivo gestito
Gestione dei criteri
Visualizzazione dell'elenco di criteri
Creazione di un criterio
Impostazioni generali dei criteri
Modifica di un criterio

Abilitazione e disabilitazione di un'opzione di ereditarietà dei criteri
Copia di un criterio
Spostamento di un criterio
Esportazione di un criterio
Importazione di un criterio
Sincronizzazione forzata
Visualizzazione del grafico dello stato di distribuzione dei criteri
Eliminazione di un criterio
Gestione dei profili criterio
Visualizzazione dei profili di un criterio
Modifica della priorità di un profilo criterio
Creazione di un profilo criterio
Copia di un profilo criterio
Creazione di una regola di attivazione del profilo criterio
Eliminazione di un profilo criterio
Impostazioni del criterio di Network Agent
Utilizzo di Network Agent per Windows, Linux e macOS a confronto
Confronto tra le impostazioni di Network Agent in base ai sistemi operativi
Configurazione manuale del criterio di Kaspersky Endpoint Security
Configurazione di Kaspersky Security Network
Controllo dell'elenco delle reti protette dal Firewall
Disabilitazione della scansione delle unità di rete
Esclusione dei dettagli del software dalla memoria di Administration Server
Configurazione dell'accesso all'interfaccia di Kaspersky Endpoint Security for Windows nelle workstation
Salvataggio degli eventi di criteri importanti nel database dell'Administration Server
Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security
Finestra Kaspersky Security Network (KSN)
Informazioni su KSN
Impostazione dell'accesso a KSN
Abilitazione e disabilitazione dell'utilizzo di KSN
Visualizzazione dell'Informativa KSN accettata
Accettazione di un'Informativa KSN aggiornata
Verifica per stabilire se il punto di distribuzione funziona come server proxy KSN
Gestione di attività
Informazioni sulle attività
Informazioni sull'ambito dell'attività
Creazione di un'attività
Avvio manuale di un'attività
Visualizzazione dell'elenco delle attività
Impostazioni generali delle attività
Esportazione di un'attività
Importazione di un'attività
Avvio della Procedura guidata per la modifica della password delle attività
Passaggio 1. Immissione delle credenziali
Passaggio 2. Selezione di un'azione da eseguire
Passaggio 3. Visualizzazione dei risultati
Visualizzazione dei risultati dell'esecuzione delle attività memorizzati in Administration Server
Tag applicazione

Creazione di un tag applicazione
Ridenominazione di un tag applicazione
Assegnazione di tag a un'applicazione
Rimozione dei tag assegnati a un'applicazione
Eliminazione di un tag applicazione
Concessione dell'accesso offline al dispositivo esterno bloccato da Controllo Dispositivi
Utilizzo dell'utilità klscflag per aprire la porta 13291
Registrazione dell'applicazione Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center Web Console
Gestione di utenti e ruoli utente
Informazioni sugli account utente
Informazioni sui ruoli utente
Configurazione dei diritti di accesso alle funzionalità dell'applicazione. Controllo dell'accesso basato sui ruoli
Diritti di accesso alle funzionalità dell'applicazione
Ruoli utente predefiniti
Assegnazione dei diritti di accesso a oggetti specifici
Assegnazione dei diritti di accesso a utenti e gruppi
Aggiunta di un account di un utente interno
Creazione di un gruppo di protezione
Modifica di un account di un utente interno
Modifica di un gruppo di protezione
Assegnazione di un ruolo a un utente o un gruppo di protezione
Aggiunta di account utente a un gruppo di protezione interno
Assegnazione di un utente come proprietario dispositivo
Abilitazione della protezione dell'account dalle modifiche non autorizzate
Verifica in due passaggi
Scenario: Configurazione della verifica in due passaggi per tutti gli utenti
Informazioni sulla verifica in due passaggi per un account
Abilitazione della verifica in due passaggi per il proprio account
Abilitazione della verifica in due passaggi richiesta per tutti gli utenti
Disabilitazione della verifica in due passaggi per un account utente
Disabilitazione della verifica in due passaggi richiesta per tutti gli utenti
Esclusione di account dalla verifica in due passaggi
Configurazione della verifica in due passaggi per il proprio account
Impedisci ai nuovi utenti di impostare la verifica in due passaggi per se stessi
Generazione di una nuova chiave segreta
Modifica del nome dell'emittente del codice di sicurezza
Modifica del numero di tentativi di immissione della password consentiti
Eliminazione di un utente o un gruppo di protezione
Creazione di un ruolo utente
Modifica di un ruolo utente
Modifica dell'ambito di un ruolo utente
Eliminazione di un ruolo utente
Associazione dei profili criterio ai ruoli
Propagazione dei ruoli utente agli Administration Server secondari
Aggiornamento di database e applicazioni Kaspersky
Scenario: Aggiornamento periodico di database e applicazioni Kaspersky
Informazioni sull'aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky
Creazione dell'attività Scarica aggiornamenti nell'archivio dell'Administration Server

Verifica degli aggiornamenti scaricati
Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione
Aggiunta di sorgenti degli aggiornamenti per l'attività Scarica aggiornamenti nell'archivio di Administration Server
Installazione automatica degli aggiornamenti per Kaspersky Endpoint Security for Windows
Informazioni sull'utilizzo dei file diff per l'aggiornamento dei database e dei moduli del software Kaspersky
Abilitazione della funzionalità Download dei file diff
Download degli aggiornamenti tramite punti di distribuzione
Aggiornamento dei database e dei moduli software Kaspersky nei dispositivi offline
Backup e ripristino dei plug-in Web
Monitoraggio, generazione di rapporti e audit
Scenario: monitoraggio e generazione dei rapporti
Informazioni sui tipi di monitoraggio e generazione dei rapporti
Dashboard e widget
Utilizzo del dashboard
Aggiunta di widget al dashboard
Occultamento di un widget dal dashboard
Spostamento di un widget nel dashboard
Modifica delle dimensioni o dell'aspetto del widget
Modifica delle impostazioni del widget
Informazioni sulla modalità Solo dashboard
Configurazione della modalità Solo dashboard
Rapporti
Utilizzo dei rapporti
Creazione di un modello di rapporto
Visualizzazione e modifica delle proprietà dei modelli di rapporto
Esportazione di un rapporto in un file
Generazione e visualizzazione di un rapporto
Creazione di un'attività di invio dei rapporti
Eliminazione di modelli di rapporto
Eventi e selezioni di eventi
Informazioni sugli eventi in Kaspersky Security Center Linux
Eventi dei componenti di Kaspersky Security Center Linux
Struttura dei dati della descrizione del tipo di evento
Eventi di Administration Server
Eventi critici di Administration Server
Eventi di errore funzionale di Administration Server
Eventi di avviso di Administration Server
Eventi informativi di Administration Server
Eventi di Network Agent
Eventi di avviso di Network Agent
Eventi informativi di Network Agent
Utilizzo di selezioni eventi
Creazione di una selezione eventi
Modifica di una selezione eventi
Visualizzazione di un elenco di una selezione eventi
Esportazione di una selezione di eventi
Importazione di una selezione di eventi
Visualizzazione dei dettagli di un evento

Esportazione degli eventi in un file
Visualizzazione della cronologia di un oggetto da un evento
Eliminazione di eventi
Eliminazione di selezioni eventi
Impostazione del periodo di archiviazione per un evento
Blocco degli eventi frequenti
Informazioni sul blocco degli eventi frequenti
Gestione del blocco degli eventi frequenti
Rimozione del blocco degli eventi frequenti
Elaborazione e archiviazione di eventi in Administration Server
Notifiche e stati del dispositivo
Utilizzo delle notifiche
Visualizzazione delle notifiche sullo schermo
Informazioni sugli stati dei dispositivi
Configurazione dell'invio delle notifiche
Testing delle notifiche
Notifiche degli eventi visualizzate dall'esecuzione di un file eseguibile
Annunci Kaspersky
Informazioni sugli annunci di Kaspersky
Configurazione delle impostazioni per gli annunci di Kaspersky
Disabilitazione degli annunci di Kaspersky
Esportazione di eventi nei sistemi SIEM
Configurazione dell'esportazione di eventi nei sistemi SIEM
Prima di iniziare
Informazioni sull'esportazione degli eventi
Informazioni sulla configurazione dell'esportazione di eventi in un sistema SIEM
Contrassegno degli eventi per l'esportazione nei sistemi SIEM in formato Syslog
Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog
Contrassegno di eventi generici per l'esportazione nel formato Syslog
Informazioni sull'esportazione degli eventi utilizzando il formato Syslog
Configurazione di Kaspersky Security Center Linux per l'esportazione degli eventi nel sistema SIEM
Esportazione degli eventi direttamente dal database
Esecuzione di una query SQL tramite l'utilità klsql2
Esempio di una query SQL nell'utilità klsql2
Visualizzazione del nome del database di Kaspersky Security Center Linux
Visualizzazione dei risultati dell'esportazione
Gestione delle revisioni degli oggetti
Rollback di un oggetto a una revisione precedente
Eliminazione di oggetti
Download ed eliminazione dei file da Quarantena e Backup
Download dei file da Quarantena e Backup
Informazioni sulla rimozione di oggetti dagli archivi Quarantena, Backup o Minacce attive
Diagnostica remota dei dispositivi client
Apertura della finestra di diagnostica remota
Abilitazione e disabilitazione del tracciamento per le applicazioni
Download dei file di traccia di un'applicazione
Eliminazione dei file di traccia
Download delle impostazioni delle applicazioni

Download delle informazioni di sistema da un dispositivo client
Download dei registri eventi
Avvio, arresto, riavvio dell'applicazione
Esecuzione della diagnostica remota di Kaspersky Security Center Linux Network Agent e download dei risultati
Esecuzione di un'applicazione in un dispositivo client
Generazione di un file di dump per un'applicazione
Esecuzione della diagnostica remota in un dispositivo client basato su Linux
Gestione delle applicazioni e dei file eseguibili di terzi nei dispositivi client
Utilizzo di Controllo Applicazioni per gestire i file eseguibili
Modalità e categorie di Controllo Applicazioni
Recupero e visualizzazione di un elenco delle applicazioni installate nei dispositivi client
Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client
Creazione di una categoria di applicazioni con contenuto aggiunto manualmente
Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati
Creazione di una categoria di applicazioni che include i file eseguibili in una cartella selezionata
Visualizzazione dell'elenco delle categorie di applicazioni
Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows
Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni
Guida di riferimento API
Procedure consigliate per i provider di servizi
Pianificazione della distribuzione di Kaspersky Security Center Linux
Concessione dell'accesso via Internet all'Administration Server
Configurazione standard di Kaspersky Security Center Linux
Informazioni sui punti di distribuzione
Gerarchia di Administration Server
Administration Server virtuali
Distribuzione e configurazione iniziale
Raccomandazioni sull'installazione di Administration Server
Creazione degli account per i servizi di Administration Server in un cluster di failover
Selezione di un DBMS
Specificazione dell'indirizzo dell'Administration Server
Distribuzione di Network Agent e delle applicazioni di protezione
Configurazione della protezione nella rete di un'organizzazione client
Configurazione manuale del criterio di Kaspersky Endpoint Security
Configurazione del criterio nella sezione Protezione minacce avanzata
Configurazione del criterio nella sezione Protezione minacce essenziale
Configurazione del criterio nella sezione Impostazioni generali
Configurazione del criterio nella sezione Configurazione eventi
Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security
Configurazione manuale dell'attività di gruppo per la scansione di un dispositivo con Kaspersky Endpoint Security
Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti
Configurazione manuale dell'attività di gruppo per l'installazione degli aggiornamenti e la correzione delle vulnerabilità
Creazione di una struttura di gruppi di amministrazione e assegnazione dei punti di distribuzione
Configurazione del client MSP standard: singola sede
Configurazione del client MSP standard: più sedi remote di piccole dimensioni
Gerarchia di criteri tramite i profili criterio
Gerarchia dei criteri
Profili criterio

Attività
Regole di spostamento dei dispositivi
Classificazione del software
Backup e ripristino delle impostazioni di Administration Server
Un dispositivo con Administration Server è inutilizzabile
Le impostazioni di Administration Server o il database sono danneggiati
Informazioni sui profili di connessione per gli utenti fuori sede
Accesso remoto ai dispositivi gestiti
Utilizzo dell'opzione "Non eseguire la disconnessione da Administration Server" per garantire connettività continua tra un dispositivo gestito e Administration Server
Informazioni sul controllo del tempo di connessione tra un dispositivo e Administration Server
Informazioni sulla sincronizzazione forzata
Guida per il dimensionamento
Informazioni sulla guida
Calcoli per gli Administration Server
Calcolo delle risorse hardware per Administration Server
Requisiti hardware per il DBMS e l'Administration Server
Calcolo dello spazio del database
Calcolo dello spazio su disco
Calcolo del numero e configurazione degli Administration Server
Suggerimenti per la connessione di macchine virtuali dinamiche a Kaspersky Security Center
Calcoli per punti di distribuzione e gateway di connessione
Requisiti per un punto di distribuzione
Calcolo del numero e configurazione dei punti di distribuzione
Calcolo del numero di gateway di connessione
Registrazione delle informazioni sugli eventi per le attività e i criteri
Best practice per un Administration Server che gestisce un numero elevato di dispositivi
Considerazioni specifiche e impostazioni ottimali di determinate attività
Frequenza della device discovery
Attività di backup dei dati di Administration Server e attività di manutenzione dei database
Attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
Attività di inventario
Dettagli del carico di rete trasmesso fra Administration Server e dispositivi protetti
Consumo del traffico in diversi scenari
Utilizzo del traffico medio nell'arco di 24 ore
Contatta Assistenza tecnica
Come ottenere assistenza tecnica
Assistenza tecnica tramite Kaspersky CompanyAccount
Recupero dei file di dump di Administration Server
Fonti di informazioni sull'applicazione
Problemi noti
Glossario
Administration Console
Administration Server
Administration Server principale
Administration Server virtuale
Agente di Autenticazione
Aggiorna

Aggiornamento disponibile
Amministratore client
Amministratore del provider di servizi
Amministratore di Kaspersky Security Center Linux
Applicazione incompatibile
Archivio eventi
Attività
Attività di gruppo
Attività locale
Attività per dispositivi specifici
Backup dei dati di Administration Server
Cartella di backup
Certificato condiviso
Certificato di Administration Server
Chiave attiva
Chiave di licenza aggiuntiva (o di riserva)
Client di Administration Server (dispositivo client)
Criterio
Database anti-virus
Diritti di amministratore
Dispositivi gestiti
Dominio di trasmissione
File chiave
Gateway di connessione
Gestione centralizzata delle applicazioni
Gestione diretta delle applicazioni
Gruppo di amministrazione
Gruppo di ruoli
HTTPS
Impostazioni attività
Impostazioni del programma
Installazione locale
Installazione manuale
Installazione remota
JavaScript
Kaspersky Private Security Network (KPSN)
Kaspersky Security Center Linux Web Server
Kaspersky Security Center System Health Validator (SHV)
Lightweight Nagent (LWNGT)
Livello di criticità di un evento
Negozio applicazioni
Network Agent
Network Location Awareness (NLA)
Operatore di Kaspersky Security Center
Pacchetto di installazione
Periodo licenza
Profilo
Profilo di configurazione

Profilo di provisioning
Proprietario dispositivo
Protezione anti-virus della rete
Provider di servizi di protezione anti-virus
Punto di distribuzione
Rete perimetrale (DMZ)
Ripristino
Ripristino dei dati di Administration Server
Server degli aggiornamenti Kaspersky
SSL
Stato della protezione della rete
Stato protezione
Utenti interni
Workstation dell'amministratore
Informazioni sul codice di terze parti
Note relative ai marchi registrati

Guida di Kaspersky Security Center Linux

Nuove funzioni

- Novità

Requisiti hardware e software

- Requisiti di Administration Server
- Requisiti di Web Console
- Requisiti di Network Agent

Operazioni preliminari

- Installazione
- Avvio rapido guidato
- Distribuzione guidata della protezione

Licensing e attivazione

- Attivazione di Kaspersky Security Center Linux
- Licensing delle applicazioni gestite

Distribuzione e configurazione

- Individuazione dei dispositivi nella rete
- Regolazione di punti di distribuzione e/o gateway di connessione
- Sostituzione di applicazioni di protezione di terzi
- Applicazioni Kaspersky. Distribuzione centralizzata
- Configurazione della protezione di rete

- Applicazioni Kaspersky. Aggiornamento dei database e dei moduli del software

Monitoraggio

- Monitoraggio e generazione dei rapporti

Funzionalità aggiuntive

- Esportazione di eventi nei sistemi SIEM
- Guida per il dimensionamento (solo Guida in linea)

Novità

Guida di Kaspersky Security Center 15 Linux

Kaspersky Security Center Linux 15 prevede diversi miglioramenti e nuove funzionalità:

- Il polling del controller di dominio consente di eseguire il polling di un controller di dominio Microsoft Active Directory e di un controller di dominio Samba. È possibile utilizzare Administration Server o un punto di distribuzione per eseguire il polling di Microsoft Active Directory. È possibile eseguire il polling di un controller di dominio Samba solo tramite un punto di distribuzione basato su Linux. Quando si esegue il polling di un controller di dominio, Administration Server o un punto di distribuzione recuperano le informazioni sulla struttura del dominio, sugli account utente, sui gruppi di protezione e sui nomi DNS dei dispositivi inclusi nel dominio.
- Kaspersky Security Center Linux ora supporta l'utilizzo dei seguenti DBMS:
  - PostgreSQL 15.x
  - Postgres Pro 15.x
- Se si utilizza PostgreSQL o Postgres Pro come DBMS, Kaspersky Security Center Linux supporta fino a 50.000 dispositivi gestiti.
- Migrazione da Kaspersky Security Center Windows a Kaspersky Security Center Linux. È possibile eseguire una migrazione guidata degli oggetti di Kaspersky Security Center, comprese le attività, i criteri e la struttura dei gruppi di amministrazione. Successivamente, è possibile spostare i dispositivi gestiti importati in modo che siano gestiti da Kaspersky Security Center Linux.
- Kaspersky Security Center Linux ora supporta l'utilizzo delle seguenti applicazioni Kaspersky:
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Embedded Systems Security for Windows
  - Kaspersky Embedded Systems Security for 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
- Diagnostica remota dei dispositivi gestiti basati su Windows e Linux.
- Componente Controllo Applicazioni migliorato. È ora possibile creare una categoria di applicazioni in base all'elenco di file eseguibili da una cartella selezionata o in base a una categoria di applicazioni Kaspersky. Quindi, è possibile specificare se consentire o bloccare le applicazioni della categoria creata nell'organizzazione.
- Esportazione e importazione di selezioni di eventi. È possibile esportare una selezione di eventi definita dall'utente e le relative impostazioni in un file KLO, quindi importare la selezione di eventi salvata in Kaspersky Security Center Windows o Kaspersky Security Center Linux.

- Nel Rapporto sulle minacce, è ora possibile aprire una catena di sviluppo delle minacce facendo clic sul collegamento **Visualizza avviso**.

- Kaspersky Security Center Linux ora supporta la tecnologia cluster. Se un gruppo di amministrazione contiene cluster o array di server, la pagina **Dispositivi gestiti** mostra due schede: una per i singoli dispositivi e una per i cluster e gli array di server. Dopo che i dispositivi gestiti vengono rilevati come nodi del cluster, il cluster viene aggiunto come oggetto singolo alla scheda **Cluster e array di server**. I nodi del cluster sono elencati nella scheda **Dispositivi**, insieme ad altri dispositivi gestiti.

- Il supporto per alcune piattaforme da parte di Kaspersky Security Center Linux è terminato perché queste piattaforme non sono più supportate dai relativi fornitori.

Guida di Kaspersky Security Center 14.2 Linux

Kaspersky Security Center Linux 14.2 prevede diversi miglioramenti e nuove funzionalità:

- In un Gerarchia di Administration Server, un server di amministrazione basato su Linux può ora fungere da server primario e può gestire server basati su Linux o Windows fungendo da server secondario.

- Kaspersky Security Center Linux ora supporta Kaspersky Security Network (KSN), Servizio proxy KSN e Kaspersky Private Security Network (KPSN).

- Kaspersky Security Center Linux ora supporta Kaspersky Endpoint Security for Windows come applicazione gestita.

  L'installazione remota di Network Agent per Windows nei dispositivi client è possibile solo utilizzando gli strumenti del sistema operativo tramite i punti di distribuzione basati su Windows.

- I dati nei dispositivi gestiti basati su Windows possono ora essere criptati per ridurre il rischio di perdita involontaria di dati sensibili e aziendali in caso di furto o smarrimento di un laptop o disco rigido. Questa funzionalità è implementata tramite Kaspersky Endpoint Security for Windows.

- Kaspersky Security Center Linux consente di scaricare e aggiornare sia i pacchetti di distribuzione delle applicazioni Kaspersky che i plug-in Web di gestione direttamente nell'interfaccia utente di Kaspersky Security Center Linux.

- Per impostazione predefinita, le informazioni sulle applicazioni installate nei dispositivi gestiti basati su Linux e Windows vengono inviate all'Administration Server.

- L'accesso ai server di Kaspersky viene ora verificato automaticamente. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza il DNS pubblico.

- I dati sensibili trasferiti tra l'Administration Server primario, gli Administration Server secondari e i Network Agent sono ora protetti con l'algoritmo di criptaggio AES.

- I diritti utente su un Administration Server virtuale sono disponibili per la configurazione in qualsiasi momento, indipendentemente dall'Administration Server primario. Inoltre, è possibile assegnare agli utenti del server primario i diritti per gestire un server virtuale.

- Kaspersky Security Center Linux ora supporta l'utilizzo dei seguenti DBMS:

  - PostgreSQL 13.x

  - PostgreSQL 14.x

  - Postgres Pro 13.x (tutte le edizioni)

- Postgres Pro 14.x (tutte le edizioni)

- È possibile utilizzare Kaspersky Security Center Web Console per esportare criteri e attività in un file, e quindi importare i criteri e le attività in Kaspersky Security Center Windows o Kaspersky Security Center Linux.

- L'opzione **Non utilizzare il server proxy** è stata rimossa dalle seguenti attività:

  - *Scarica aggiornamenti nell'archivio dell'Administration Server*

  - *Scarica aggiornamenti negli archivi dei punti di distribuzione*

Guida di Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux prevede diversi miglioramenti e nuove funzionalità:

- Oltre all'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, i database anti-virus per le applicazioni di protezione Kaspersky possono ora essere scaricati tramite l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

- I database anti-virus e i moduli dell'applicazione nei dispositivi gestiti possono essere propagati e aggiornati tramite Administration Server o punti di distribuzione. È possibile scegliere uno schema di aggiornamento ottimale per la propria organizzazione, per ridurre il carico sull'Administration Server e ottimizzare il traffico dei dati sulla rete aziendale.

- Kaspersky Security Center Linux scarica dai server di aggiornamento Kaspersky solo gli aggiornamenti richiesti dalle applicazioni di protezione Kaspersky. In questo modo, si riduce la dimensione dei dati scaricati.

- Ora è possibile utilizzare le funzionalità dei file diff per scaricare database anti-virus e moduli software. Un file diff descrive le differenze tra due versioni di un file di un database o un modulo software. L'utilizzo dei file diff riduce il traffico all'interno della rete aziendale, poiché i file diff occupano meno spazio rispetto ai file completi di database e moduli software.

- È stata aggiunta l'attività di *Verifica aggiornamenti*. Utilizzando questa attività, è possibile verificare automaticamente l'operatività e gli errori degli aggiornamenti scaricati prima di installare gli aggiornamenti nei dispositivi gestiti.

- Kaspersky Security Center Linux ora supporta Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 come applicazione gestita.

Informazioni su Kaspersky Security Center Linux

Questa sezione contiene informazioni sulla funzione di Kaspersky Security Center Linux, sui relativi componenti e funzionalità principali e sulle modalità di acquisto di Kaspersky Security Center.

Kaspersky Security Center Linux (denominato anche Kaspersky Security Center) è progettato per distribuire e gestire la protezione dei dispositivi client utilizzando Administration Server basato su Linux.

Kaspersky Security Center Linux consente all'utente di installare le applicazioni di protezione Kaspersky nei dispositivi in una rete aziendale, eseguire in remoto attività di scansione e aggiornamento e gestire i criteri di sicurezza delle applicazioni gestite. In qualità di amministratore, è possibile utilizzare una dashboard dettagliata che fornisce una panoramica degli stati dei dispositivi aziendali, rapporti dettagliati e impostazioni granulari nei criteri di protezione.

Rispetto a Kaspersky Security Center con Administration Server basato su Windows®, Kaspersky Security Center Linux dispone di un set di funzionalità diverso.

L'applicazione Kaspersky Security Center Linux è destinata agli amministratori di reti aziendali e ai dipendenti responsabili della protezione dei dispositivi in un'ampia gamma di organizzazioni.

Utilizzando Kaspersky Security Center è possibile eseguire quanto segue:

- Creare una gerarchia di Administration Server per gestire la rete dell'organizzazione, nonché le reti di filiali remote o organizzazioni client.

  Un'*organizzazione client* è un'organizzazione la cui protezione anti-virus viene assicurata da un provider di servizi.

- Creare una gerarchia di gruppi di amministrazione per gestire una selezione di dispositivi client come una singola unità.

- Gestire un sistema di protezione anti-virus basato sulle applicazioni Kaspersky.

- Eseguire l'installazione remota delle applicazioni Kaspersky e di altri fornitori di software.

- Eseguire la distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky nei dispositivi client, monitorarne l'utilizzo e rinnovare le licenze.

- Ricevere statistiche e rapporti sull'esecuzione delle applicazioni e dei dispositivi.

- Ricevere notifiche relative agli eventi critici durante l'esecuzione delle applicazioni Kaspersky.

- Gestire il criptaggio delle informazioni archiviate in unità rimovibili e dischi rigidi di dispositivi basati su Windows.

- Gestire l'accesso degli utenti ai dati criptati nei dispositivi basati su Windows.

- Eseguire l'inventario dell'hardware connesso alla rete dell'organizzazione.

- Gestire in modo centralizzato il file spostati in Quarantena o Backup dalle applicazioni di protezione, nonché gestire i file per cui l'elaborazione da parte delle applicazioni di protezione è stata rimandata.

È possibile acquistare Kaspersky Security Center Linux tramite Kaspersky (ad esempio, all'indirizzo https://www.kaspersky.it) o tramite aziende partner.

Se Kaspersky Security Center Linux viene acquistato tramite Kaspersky, è possibile copiare l'applicazione dal nostro sito Web. Le informazioni richieste per l'attivazione dell'applicazione vengono inviate tramite e-mail una volta elaborato il pagamento.

Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Requisiti hardware e software

- Requisiti di Administration Server
- Requisiti di Web Console
- Requisiti di Network Agent

Requisiti di Administration Server

Requisiti hardware minimi:

- CPU con frequenza operativa di 1,4 GHz o superiore.
- RAM: 4 GB.
- Spazio su disco disponibile: 10 GB richiesti per la cartella in cui sono archiviati i dati di Administration Server (/var/opt/kaspersky/klnagent_srv).

Sono supportati i seguenti sistemi operativi:

- Debian GNU/Linux 10.x (Buster) 64 bit
- Debian GNU/Linux 11.x (Bullseye) 64 bit
- Debian GNU/Linux 12 (Bookworm) 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
- CentOS 7.x 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 (tutti i Service Pack) 64 bit
- SUSE Linux Enterprise Server 15 (tutti i Service Pack) 64 bit

- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.6) 64 bit
- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.7) 64 bit
- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.8) 64 bit
- Astra Linux Common Edition (aggiornamento operativo 2.12) 64 bit
- ALT SP Server 10 64 bit
- ALT Server 10 64 bit
- ALT Server 9.2 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
- ROSA COBALT 7.9 64 bit

Si consiglia di utilizzare il file system EXT4 con le impostazioni predefinite.

Sono supportate le seguenti piattaforme di virtualizzazione:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64 bit
- Microsoft Hyper-V Server 2012 R2 64 bit
- Microsoft Hyper-V Server 2016 64 bit
- Microsoft Hyper-V Server 2019 64 bit

- Microsoft Hyper-V Server 2022 64 bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- Macchina virtuale basata su kernel (tutti i sistemi operativi Linux supportati dal server di amministrazione)

Sono supportati i seguenti server di database (può essere installato su un dispositivo diverso):

- MySQL 5.7 Community 32 bit/64 bit
- MySQL 8.0 32 bit/64 bit
- MariaDB 10.1 (build 10.1.30 e versioni successive) 32 bit/64 bit
- MariaDB 10.3 (build 10.3.22 e versioni successive) 32 bit/64 bit
- MariaDB 10.4 (build 10.4.20 e versioni successive) 32 bit/64 bit
- MariaDB 10.5 (build 10.5.27 e versioni successive) 32 bit/64 bit
- MariaDB 10.6 (build 10.6.20 e versioni successive) 32 bit/64 bit
- MariaDB 10.11 (build 10.11.10 e versioni successive) 32 bit/64 bit
- Cluster MariaDB Galera 10.3 a 32 bit/64 bit con motore di archiviazione InnoDB
- PostgreSQL 13.x 64 bit
- PostgreSQL 14.x 64 bit
- PostgreSQL 15.x 64 bit
- Postgres Pro 13.x 64 bit (tutte le edizioni)
- Postgres Pro 14.x 64-bit (tutte le edizioni)
- Postgres Pro 15.x 64 bit (tutte le edizioni)
- Platform V Pangolin 5.4.0 64 bit
- Jatoba 4 64 bit

Requisiti di Web Console

Kaspersky Security Center Web Console Server

Requisiti hardware minimi:

- CPU: 4 core, frequenza operativa di 2,5 GHz.
- RAM: 8 GB.
- Spazio su disco disponibile: 40 GB richiesti per la cartella in cui sono archiviati i dati di Administration Server (/var/opt/kaspersky).

Uno dei seguenti sistemi operativi (solo versioni a 64 bit):

- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 12 (Bookworm)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- 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 (tutti i Service Pack)
- SUSE Linux Enterprise Server 15 (tutti i Service Pack)
- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.6)
- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.7)
- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.8) 64 bit
- Astra Linux Common Edition (aggiornamento operativo 2.12)
- ALT SP Server 10
- ALT Server 10
- ALT Server 9.2
- 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
- ROSA COBALT 7.9
- Macchina virtuale basata su kernel (tutti i sistemi operativi Linux supportati da Kaspersky Security Center Web Console Server)

Dispositivi client

Per un dispositivo client, l'utilizzo di Kaspersky Security Center Web Console richiede solo un browser.

La risoluzione minima dello schermo è 1366x768 pixel.

I requisiti hardware e software relativi al dispositivo sono identici a quelli del browser utilizzato per Kaspersky Security Center Web Console.

Browser:

- Google Chrome versione 100.0.4896.88 o successiva (build ufficiale)
- Microsoft Edge versione 100 o successiva
- Safari 15 su macOS
- "Yandex" Browser 23.5.0.2271 o versione successiva
- Mozilla Firefox Extended Support Release 102.0 o versione successiva

Requisiti di Network Agent

Requisiti hardware minimi:

- CPU con frequenza operativa di 1 GHz o superiore. Per un sistema operativo a 64 bit, la frequenza minima della CPU è di 1.4 GHz.
- RAM: 512 MB.
- Spazio disponibile su disco: 1 GB.

Requisito software per dispositivi basati su Linux: è necessario installare l'interprete Perl versione 5.10 o successiva.

Sono supportati i seguenti sistemi operativi:

- Microsoft Windows Embedded POSReady 2009 con il Service Pack più recente 32 bit
- Microsoft Windows Embedded 7 Standard con 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 versione 1703 32 bit/64 bit
- Microsoft Windows 10 IoT Enterprise versione 1709 32 bit/64 bit
- Microsoft Windows 10 IoT Enterprise versione 1803 32 bit/64 bit
- Microsoft Windows 10 IoT Enterprise versione 1809 32 bit/64 bit
- Microsoft Windows 10 20H2 IoT Enterprise 32 bit/64 bit
- Microsoft Windows 10 21H2 IoT Enterprise 32 bit/64 bit
- Microsoft Windows 10 IoT Enterprise 32 bit/64 bit
- Microsoft Windows 10 IoT Enterprise versione 1909 32 bit/64 bit
- Microsoft Windows 10 IoT Enterprise LTSC 2021 32 bit/64 bit
- Microsoft Windows 10 IoT Enterprise versione 1607 32 bit/64 bit
- Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32 bit/64 bit
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32 bit/64 bit
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32 bit/64 bit
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32 bit/64 bit
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32 bit/64 bit
- Microsoft Windows 10 Home RS4 (aggiornamento di aprile 2018, 17134) 32 bit/64 bit
- Microsoft Windows 10 Pro RS4 (aggiornamento di aprile 2018, 17134) 32 bit/64 bit
- Microsoft Windows 10 Pro for Workstations RS4 (aggiornamento di aprile 2018, 17134) 32 bit/64 bit
- Microsoft Windows 10 Enterprise RS4 (aggiornamento di aprile 2018, 17134) 32 bit/64 bit
- Microsoft Windows 10 Education RS4 (aggiornamento di aprile 2018, 17134) 32 bit/64 bit

- Microsoft Windows 10 Home RS5 (ottobre 2018) 32 bit/64 bit
- Microsoft Windows 10 Pro RS5 (ottobre 2018) 32 bit/64 bit
- Microsoft Windows 10 Pro for Workstations RS5 (ottobre 2018) 32 bit/64 bit
- Microsoft Windows 10 Enterprise RS5 (ottobre 2018) 32 bit/64 bit
- Microsoft Windows 10 Education RS5 (ottobre 2018) 32 bit/64 bit
- Microsoft Windows 10 Home 19H1 32 bit/64 bit
- Microsoft Windows 10 Pro 19H1 32 bit/64 bit
- Microsoft Windows 10 Pro for Workstations 19H1 32 bit/64 bit
- Microsoft Windows 10 Enterprise 19H1 32 bit/64 bit
- Microsoft Windows 10 Education 19H1 32 bit/64 bit
- Microsoft Windows 10 Home 19H2 32 bit/64 bit
- Microsoft Windows 10 Pro 19H2 32 bit/64 bit
- Microsoft Windows 10 Pro for Workstations 19H2 32 bit/64 bit
- Microsoft Windows 10 Enterprise 19H2 32 bit/64 bit
- Microsoft Windows 10 Education 19H2 32 bit/64 bit
- Microsoft Windows 10 Home 20H1 (aggiornamento di maggio 2020) 32 bit/64 bit
- Microsoft Windows 10 Pro 20H1 (aggiornamento di maggio 2020) 32 bit/64 bit
- Microsoft Windows 10 Enterprise 20H1 (aggiornamento di maggio 2020) 32 bit/64 bit
- Microsoft Windows 10 Education 20H1 (aggiornamento di maggio 2020) 32 bit/64 bit
- Microsoft Windows 10 Home 20H2 (aggiornamento di ottobre 2020) 32 bit/64 bit
- Microsoft Windows 10 Pro 20H2 (aggiornamento di ottobre 2020) 32 bit/64 bit
- Microsoft Windows 10 Enterprise 20H2 (aggiornamento di ottobre 2020) 32 bit/64 bit
- Microsoft Windows 10 Education 20H2 (aggiornamento di ottobre 2020) 32 bit/64 bit
- Microsoft Windows 10 Home 21H1 (aggiornamento di maggio 2021) 32 bit/64 bit
- Microsoft Windows 10 Pro 21H1 (aggiornamento di maggio 2021) 32 bit/64 bit
- Microsoft Windows 10 Enterprise 21H1 (aggiornamento di maggio 2021) 32 bit/64 bit
- Microsoft Windows 10 Education 21H1 (aggiornamento di maggio 2021) 32 bit/64 bit
- Microsoft Windows 10 Home 21H2 (aggiornamento di ottobre 2021) 32 bit / 64 bit

- Microsoft Windows 10 Pro 21H2 (aggiornamento di ottobre 2021) 32 bit / 64 bit
- Microsoft Windows 10 Enterprise 21H2 (aggiornamento di ottobre 2021) 32 bit / 64 bit
- Microsoft Windows 10 Education 21H2 (aggiornamento di ottobre 2021) 32 bit / 64 bit
- Microsoft Windows 10 Home 22H2 (aggiornamento di ottobre 2023) 32 bit/64 bit
- Microsoft Windows 10 Pro 22H2 (aggiornamento di ottobre 2023) 32 bit/64 bit
- Microsoft Windows 10 Enterprise 22H2 (aggiornamento di ottobre 2023) 32 bit/64 bit
- Microsoft Windows 10 Education 22H2 (aggiornamento di ottobre 2023) 32 bit/64 bit
- Microsoft Windows 11 Home 64 bit
- Microsoft Windows 11 Pro 64 bit
- Microsoft Windows 11 Enterprise 64 bit
- Microsoft Windows 11 Education 64 bit
- Microsoft Windows 11 22H2
- Microsoft Windows 8.1 Pro 32 bit/64 bit
- Microsoft Windows 8.1 Enterprise 32 bit/64 bit
- Microsoft Windows 8 Pro 32 bit/64 bit
- Microsoft Windows 8 Enterprise 32 bit/64 bit
- Microsoft Windows 7 Professional con Service Pack 1 e versioni successive 32 bit/64 bit
- Microsoft Windows 7 Enterprise / Ultimate con Service Pack 1 e versioni successive 32 bit/64 bit
- Microsoft Windows 7 Home Basic/Premium con Service Pack 1 e versioni successive 32 bit/64 bit
- Microsoft Windows XP Professional con Service Pack 2 a 32 bit/64 bit (supportato solo da Network Agent versione 10.5.1781)
- Microsoft Windows XP Professional con Service Pack 3 e versioni successive 32 bit (supportato da Network Agent versione 14.0.0.20023)
- Microsoft Windows XP Professional per sistemi integrati con Service Pack 3 32 bit (supportato da Network Agent versione 14.0.0.20023)
- Windows MultiPoint Server 2011 Standard/Premium 64 bit
- Windows Server 2003 SP1 a 32/64 bit (supportato solo da Network Agent versione 10.5.1781, che è possibile richiedere tramite l'Assistenza tecnica)
- Windows Server 2008 Foundation con Service Pack 2 32 bit/64 bit
- Windows Server 2008 con Service Pack 2 (tutte le edizioni) 32 bit/64 bit

- Windows Server 2008 R2 Datacenter con Service Pack 1 e versioni successive 64 bit
- Windows Server 2008 R2 Enterprise con Service Pack 1 e versioni successive 64 bit
- Windows Server 2008 R2 Foundation con Service Pack 1 e versioni successive 64 bit
- Windows Server 2008 R2 Core Mode con Service Pack 1 e versioni successive 64 bit
- Windows Server 2008 R2 Standard con Service Pack 1 e versioni successive 64 bit
- Windows Server 2008 R2 con Service Pack 1 (tutte le edizioni) 64 bit
- Windows Server 2012 Server Core 64 bit
- Windows Server 2012 Datacenter 64 bit
- Windows Server 2012 Essentials 64 bit
- Windows Server 2012 Foundation 64 bit
- Windows Server 2012 Standard 64 bit
- Windows Server 2012 R2 Server Core 64 bit
- Windows Server 2012 R2 Datacenter 64 bit
- Windows Server 2012 R2 Essentials 64 bit
- Windows Server 2012 R2 Foundation 64 bit
- Windows Server 2012 R2 Standard 64 bit
- Windows Server 2016 Datacenter (LTSB) 64 bit
- Windows Server 2016 Standard (LTSB) 64 bit
- Windows Server 2016 Server Core (Installation Option) (LTSB) 64 bit
- Windows Server 2019 Standard 64 bit
- Windows Server 2019 Datacenter 64 bit
- Windows Server 2019 Core 64 bit
- Windows Server 2022 Standard 64 bit
- Windows Server 2022 Datacenter 64 bit
- Windows Server 2022 Core 64 bit
- 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) 32 bit/64 bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 32 bit/64 bit
- Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bit
- CentOS 7.x 64 bit
- CentOS Stream 9 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 (tutti i Service Pack) 64 bit
- SUSE Linux Enterprise Server 15 (tutti i Service Pack) 64 bit
- SUSE Linux Enterprise Desktop 15 con Service Pack 3 ARM 64 bit
- openSUSE 15 64 bit
- EulerOS 2.0 SP8 ARM 64 bit
- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.6) 64 bit
- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.7) 64 bit
- Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.8) 64 bit
- Astra Linux Common Edition (aggiornamento operativo 2.12) 64 bit
- Astra Linux Special Edition RUSB.10152-02 (aggiornamento operativo 4.7) ARM 64 bit
- ALT SP Server 10 64 bit
- ALT SP Workstation 10 64 bit
- ALT Server 10 64 bit
- ALT Server 9.2 64 bit
- ALT Workstation 9.2 32 bit/64 bit
- ALT Workstation 10 32 bit/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

- 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
- AlterOS 7.5 e versioni successive 64 bit
- GosLinux IC6 64 bit
- RED OS 7.3 Server 64 bit
- RED OS 7.3 Certified Edition 64 bit
- ROSA COBALT 7.9 64 bit
- ROSA CHROME 12 64 bit
- macOS 11.x
- macOS 12.x
- macOS 13.x
- macOS 14.x
  Per Network Agent è supportata anche l'architettura Apple Silicon (M1), così come Intel.

Sono supportate le seguenti piattaforme di virtualizzazione:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- VMware Workstation 16 Pro
- VMware Workstation 17 Pro
- Microsoft Hyper-V Server 2012 64 bit
- Microsoft Hyper-V Server 2012 R2 64 bit
- Microsoft Hyper-V Server 2016 64 bit

- Microsoft Hyper-V Server 2019 64 bit
- Microsoft Hyper-V Server 2022 64 bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x
- Oracle VM VirtualBox 7.x
- Macchina virtuale basata su kernel (tutti i sistemi operativi Linux supportati da Network Agent)

Nei dispositivi che eseguono Windows 10 versione RS4 o RS5, Kaspersky Security Center potrebbe non essere in grado di rilevare alcune vulnerabilità nelle cartelle in cui è abilitata la distinzione tra maiuscole e minuscole.

Prima di installare Network Agent nei dispositivi in cui viene eseguito Windows 7, Windows Server 2008, Windows Server 2008 R2 o Windows MultiPoint Server 2011, assicurarsi di aver installato l'aggiornamento di sicurezza KB3063858 per il sistema operativo Windows (Aggiornamento di sicurezza per Windows 7 (KB3063858), Aggiornamento di sicurezza per Windows 7 per sistemi basati su x64 (KB3063858), Aggiornamento di sicurezza per Windows Server 2008 (KB3063858), Aggiornamento di sicurezza per Windows Server 2008 x64 Edition (KB3063858), Aggiornamento di sicurezza per Windows Server 2008 R2 x64 Edition (KB3063858).

In Microsoft Windows XP Network Agent non potrebbe eseguire correttamente alcune operazioni.

È possibile installare o aggiornare Network Agent for Windows XP solo in Microsoft Windows XP. Le edizioni supportate di Microsoft Windows XP e le versioni corrispondenti di Network Agent sono elencate nell'elenco dei sistemi operativi supportati. È possibile scaricare la versione richiesta di Network Agent per Microsoft Windows XP da questa pagina.

Si consiglia di installare la stessa versione di Network Agent per Linux di Kaspersky Security Center Linux.

Kaspersky Security Center Linux supporta Network Agent con versioni uguali o più recenti.

Network Agent per macOS viene fornito insieme all'applicazione di protezione Kaspersky per questo sistema operativo.

Kit di distribuzione

È possibile acquistare l'applicazione nei negozi online di Kaspersky (ad esempio, all'indirizzo https://www.kaspersky.it) o tramite aziende partner.

In caso di acquisto di Kaspersky Security Center Linux da un negozio online, l'applicazione viene scaricata dal sito Web del negozio. Le informazioni richieste per l'attivazione dell'applicazione vengono inviate tramite e-mail una volta effettuato il pagamento.

Informazioni sulla compatibilità di Administration Server e Kaspersky Security Center Web Console

Si consiglia di utilizzare la versione più recente sia di Kaspersky Security Center Linux Administration Server che di Kaspersky Security Center Web Console. In caso contrario, la funzionalità di Kaspersky Security Center Linux potrebbe essere limitata.

È possibile installare e aggiornare Kaspersky Security Center Linux Administration Server e Kaspersky Security Center Web Console in modo indipendente. In questo caso, è preferibile assicurarsi che la versione installata di Kaspersky Security Center Web Console sia compatibile con la versione di Administration Server a cui ci si connette:

- Web Console incluso in Kaspersky Security Center Linux 15 supporta le seguenti versioni di Kaspersky Security Center Linux Administration Server: 15 e 14.2.
- Administration Server incluso in Kaspersky Security Center Linux 15 supporta le seguenti versioni di Kaspersky Security Center Web Console: 15 e 14.2.

Confronto tra Kaspersky Security Center basato su Windows e basato su Linux

Kaspersky fornisce Kaspersky Security Center come soluzione locale per due piattaforme: Windows e Linux. Nella soluzione basata su Windows, Administration Server è installato in un dispositivo Windows. Nella soluzione basata su Linux, la versione di Administration Server è invece progettata per l'installazione in un dispositivo Linux. Questa Guida in linea contiene informazioni su Kaspersky Security Center Linux. Per informazioni dettagliate sulla soluzione basata su Windows, fare riferimento alla Guida in linea di Kaspersky Security Center Windows.

La seguente tabella consente di confrontare le caratteristiche principali di Kaspersky Security Center come soluzione basata su Windows e come soluzione basata su Linux.

Confronto delle funzionalità di Kaspersky Security Center come soluzione basata su Windows e soluzione basata su Linux

Funzionalità o proprietà	Kaspersky Security Center 14.2 Windows	Guida di Kaspersky Security Center 15 Linux
Posizione dell'Administration Server	In locale	In locale
Posizione del DBMS (Database Management System)	In locale	In locale
Sistema operativo in cui installare Administration Server	Windows	Linux
Tipo di Administration Console	In locale e basata sul Web	Basata sul Web
Sistema operativo in cui installare l'Administration Console basata sul Web	Windows o Linux	Linux
Gerarchia di Administration Server	✓	✓
Gerarchia di gruppi di amministrazione	✓	✓

Polling della rete	✓	✓ (per intervalli IP e controller di dominio, Samba 4 Active Directory, Microsoft Active Directory)
Numero massimo di dispositivi gestiti	100.000	50.000 (con PostgreSQL e Postgres Pro)
Protezione dei dispositivi gestiti Windows, macOS e Linux	✓	✓
Protezione dei dispositivi mobili	✓	—
Protezione delle macchine virtuali	✓	✓
Protezione dell'infrastruttura cloud pubblica	✓	—
Gestione della sicurezza incentrata sul dispositivo	✓	✓
Gestione della sicurezza incentrata sull'utente	✓	✓
Criteri dell'applicazione	✓	✓
Attività per le applicazioni Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
Proxy KSN	✓	✓
Kaspersky Private Security Network	✓	✓
Distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky	✓	✓
Aggiornamento automatico dei database anti-virus	✓	✓
Supporto per Administration Server virtuali	✓	✓
Installazione di aggiornamenti software di terze parti e correzione delle vulnerabilità del software di terze parti	✓	— (solo utilizzando un'attività di installazione remota)
Notifiche sugli eventi che si sono verificati nei dispositivi gestiti	✓	✓
Creazione e gestione degli account utente	✓	✓
Accesso alla console utilizzando l'autenticazione del dominio	✓	✓ (Single Sign-On non supportato)
Integrazione con i sistemi SIEM	✓	✓ (utilizzando solo Syslog)
Monitoraggio dello stato di criteri e attività	✓	✓
Distribuzione del cluster di failover Kaspersky Security Center	✓	✓
Installazione di Administration Server in un cluster di failover di Windows Server	✓	—
Utilizzo di SNMP per l'invio delle statistiche di Administration Server ad applicazioni di terzi	✓	—
Diagnostica remota dei dispositivi client	✓	✓
Connessione remota al desktop di un dispositivo client	✓	—
Gestione delle revisioni degli oggetti	✓	—
Aggiornamento automatico delle applicazioni Kaspersky	✓	—
Distribuzione di sistemi operativi nei dispositivi client	✓	—
Server Web per la pubblicazione di pacchetti di installazione e altri file	✓	—
Visualizzazione e utilizzo degli avvisi rilevati da Kaspersky Endpoint Detection and Response Optimum	✓	✓
Utilizzo di Administration Server come server WSUS	✓	—
Integrazione con Kaspersky Managed Detection and Response	✓	—
Supporto di Controllo adattivo delle anomalie	✓	—

Supporto di cluster e array di server nei gruppi di amministrazione	✓ (solo in Administration Console basata su MMC)	✓
Gestione di licenze di terzi	✓	–

Informazioni di Kaspersky Security Center Cloud Console

Se utilizzato come applicazione locale, Kaspersky Security Center (comprensivo di Administration Server) viene installato in un dispositivo locale e il sistema di sicurezza di rete viene gestito tramite Administration Console basata su Microsoft Management Console (disponibile solo in Kaspersky Security Center Windows) o Kaspersky Security Center Web Console.

In alternativa, è tuttavia possibile utilizzare Kaspersky Security Center come servizio cloud. In questo caso Kaspersky Security Center viene automaticamente installato e gestito dagli esperti Kaspersky nell'ambiente cloud e Kaspersky fornisce l'accesso ad Administration Server come servizio. Il sistema di sicurezza di rete viene gestito tramite Administration Console basata su cloud, denominata Kaspersky Security Center Cloud Console. Questa console ha un'interfaccia simile all'interfaccia di Kaspersky Security Center Web Console.

L'interfaccia e la documentazione di Kaspersky Security Center Cloud Console sono disponibili nelle seguenti lingue:

- Inglese
- Francese
- Tedesco
- Italiano
- Giapponese
- Portoghese (Brasile)
- Russo
- Cinese semplificato
- Spagnolo
- Spagnolo (LATAM)
- Cinese tradizionale

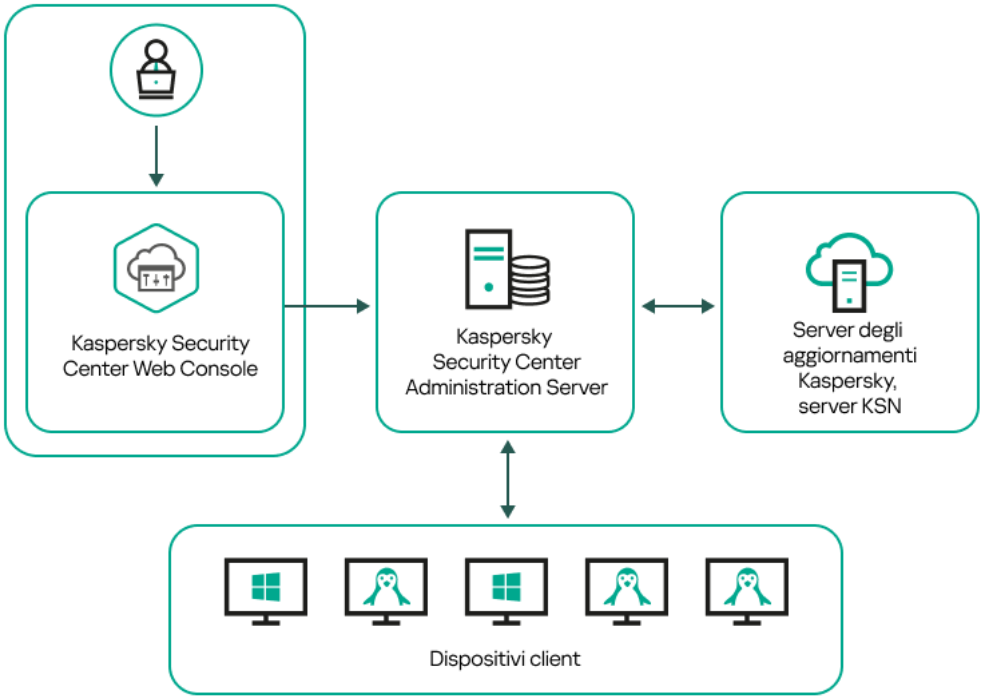
Ulteriori informazioni su Kaspersky Security Center Cloud Console e sulle relative funzionalità sono disponibili nella documentazione di Kaspersky Security Center Cloud Console e nella documentazione di Kaspersky Endpoint Security for Business.

Architettura e concetti di base

In questa sezione sono illustrati l'architettura dell'applicazione e i concetti di base relativi a Kaspersky Security Center Linux.

Architettura

Questa sezione fornisce una descrizione dei componenti di Kaspersky Security Center e la relativa interazione.



Architettura di Kaspersky Security Center Linux

Kaspersky Security Center Linux include i seguenti componenti di base:

- **Kaspersky Security Center Web Console**. Offre un'interfaccia Web per la creazione e la manutenzione del sistema di protezione di una rete di un'organizzazione client gestita tramite Kaspersky Security Center.
- **Kaspersky Security Center Administration Server** (denominato anche *Server*). Centralizza l'archiviazione delle informazioni sulle applicazioni installate nella rete aziendale e sulla relativa gestione.
- **Server di aggiornamento Kaspersky**. I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.
- **Server KSN**. Server che contengono un database Kaspersky con informazioni sempre aggiornate sulla reputazione di file, risorse Web e software. Kaspersky Security Network assicura una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliora l'efficacia di alcuni componenti della protezione e riduce la probabilità di falsi positivi.
- **Dispositivi client.** Dispositivi client dell'azienda protetti da Kaspersky Security Center Linux. Ogni dispositivo che deve essere protetto deve avere una delle applicazioni di protezione Kaspersky installate.

Diagramma di distribuzione di Kaspersky Security Center Linux Administration Server e Kaspersky Security Center Web Console

La figura seguente mostra il diagramma di distribuzione di Kaspersky Security Center Linux Administration Server e Kaspersky Security Center Web Console.

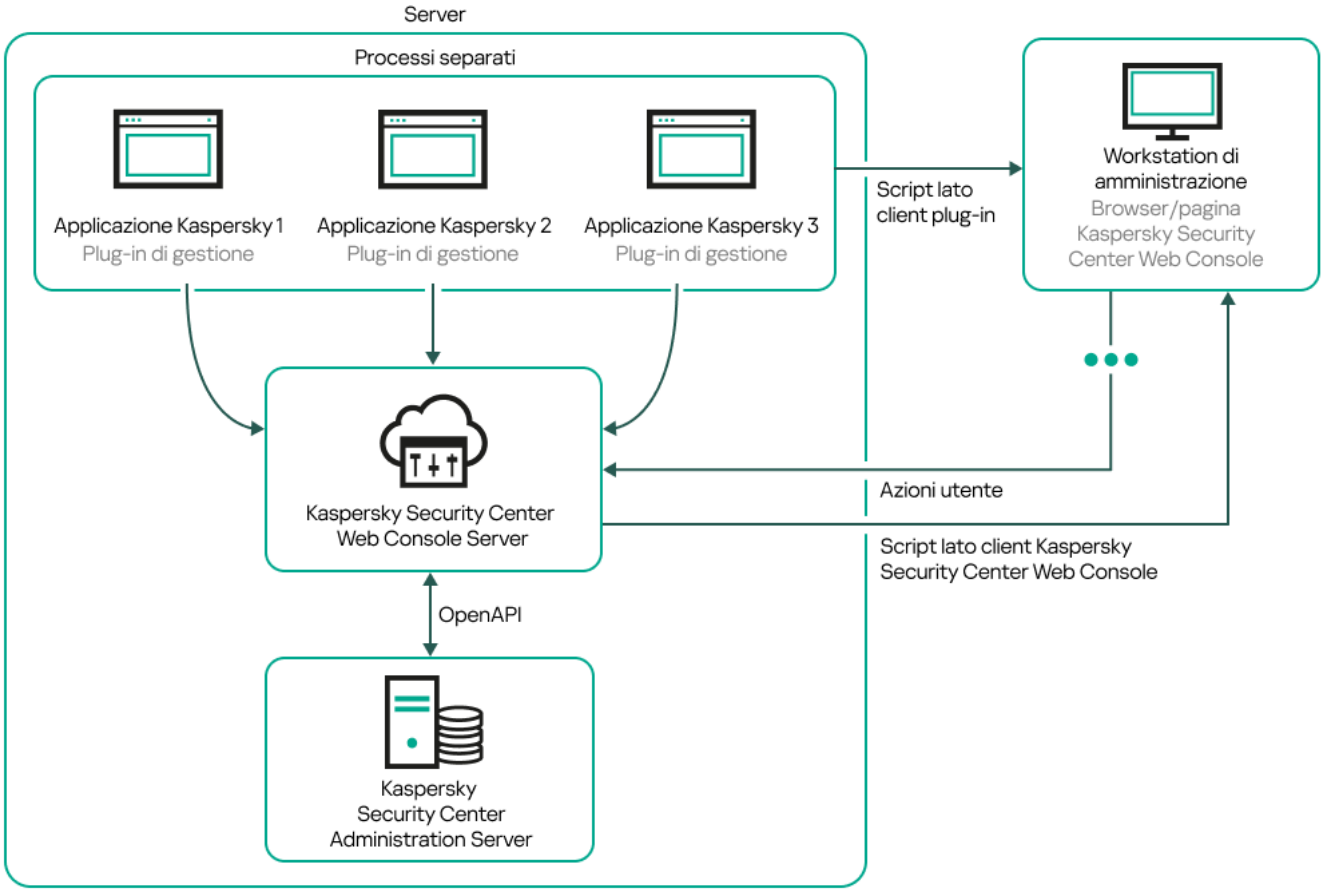


Diagramma di distribuzione di Kaspersky Security Center Linux Administration Server e Kaspersky Security Center Web Console

I plug-in di gestione per le applicazioni Kaspersky installate nei dispositivi protetti (un plug-in per ogni applicazione) vengono distribuiti insieme a Kaspersky Security Center Web Console Server.

Come amministratore, accedere a Kaspersky Security Center Web Console utilizzando un browser sulla workstation.

Quando si eseguono azioni specifiche in Kaspersky Security Center Web Console, Kaspersky Security Center Web Console Server comunica con Kaspersky Security Center Linux Administration Server tramite OpenAPI. Kaspersky Security Center Web Console Server richiede le informazioni necessarie a Kaspersky Security Center Linux Administration Server e visualizza i risultati delle operazioni in Kaspersky Security Center Web Console.

Porte utilizzate da Kaspersky Security Center Linux

Le tabelle seguenti mostrano le porte predefinite utilizzate da Administration Server e dai dispositivi client. Se si desidera, è possibile modificare ciascuno di questi numeri di porta predefiniti.

Porte utilizzate dall'Administration Server di Kaspersky Security Center Linux

Numero di porta	Nome del processo	Protocollo	Ambito della porta	Ambito

	che apre la porta			
8060	klcsweb	TCP	Trasmissione dei pacchetti di installazione pubblicati ai dispositivi client	Pubblicazione dei pacchetti di installazione. È possibile modificare il numero di porta predefinito nella sezione **Server Web** proprietà inistration Server. Questa porta è facoltativa. Per motivi di sicurezza, si consiglia di utilizzare la porta TCP 8061.
8061	klcsweb	TCP (TLS)	Trasmissione dei pacchetti di installazione pubblicati ai dispositivi client	Pubblicazione dei pacchetti di installazione. È possibile modificare il numero di porta predefinito nella sezione **Server Web** proprietà inistration Server.
13000	klserver	TCP (TLS)	Ricezione delle connessioni dai Network Agent e dagli Administration Server secondari; utilizzata anche negli Administration Server secondari per la ricezione delle connessioni dall'Administration Server primario (ad esempio, se l'Administration Server secondario è nella rete perimetrale)	Gestione dei dispositivi client e degli Administration Server secondari. È possibile modificare il numero di porta predefinito per la ricezione delle connessioni dai Network Agent durante la configurazione delle porte di connessione in fase di installazione di Kaspersky Security Center Linux; è possibile modificare il numero di porta predefinito per la ricezione delle connessioni dagli Administration Server secondari durante la creazione di una gerarchia di Administration Server.
13000	klserver	UDP	Ricezione di informazioni sui dispositivi che sono stati spenti dai Network Agent	Gestione dei dispositivi client. È possibile modificare il numero di porta predefinito nelle impostazioni del criterio di Network Agent.
13291	klserver	TCP (TLS)	Utilizzo dell'utilità klakaut per automatizzare il funzionamento di Kaspersky Security Center Linux	Utilizzo dell'utilità klakaut. L'utilità klakaut e la relativa Guida sono disponibili nella cartella di installazione di Kaspersky Security Center Linux. Questa porta è chiusa per impostazione predefinita. Se si desidera utilizzare l'utilità klakaut per automatizzare il funzionamento di Kaspersky Security Center Linux, aprire la porta 13291 tramite l'utilità klscflag.
13299	klserver	TCP (TLS)	Ricezione delle connessioni da Kaspersky Security Center Web Console ad Administration Server; ricezione delle connessioni ad Administration Server tramite OpenAPI	Gestione dell'Administration Server mediante Kaspersky Security Center Web Console; utilizzo di OpenAPI. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server (nella sottosezione **Porte di connessione** della sezione **Generale**) o durante la creazione di una gerarchia di Administration Server.
14000	klserver	TCP	Ricezione delle connessioni dai Network Agent	Gestione dei dispositivi client. È possibile modificare il numero di porta predefinito durante la configurazione delle porte di connessione nel corso dell'installazione di Kaspersky Security Center Linux o durante la connessione manuale di un dispositivo client all'Administration Server. Questa porta è facoltativa. Per motivi di sicurezza, si consiglia di utilizzare la porta TCP 1300.
13111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	ksnproxy	TCP	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server.
15111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	ksnproxy	UDP	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server.

17000	klactprx	TCP (TLS)	Ricezione delle connessioni per l'attivazione dell'applicazione dai dispositivi gestiti	Server proxy di attivazione per i dispositivi gestiti. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server (nella sottosezione **Porte aggiuntive** della sezione **Generale**).

Se si installano l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per MariaDB). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

Nella tabella seguente viene mostrata la porta utilizzata dal server Kaspersky Security Center Web Console. Può trattarsi dello stesso dispositivo in cui è installato Administration Server o di un dispositivo diverso.

Porta utilizzata da Kaspersky Security Center Web Console Server

Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta	Ambito
8080	Node.js: Server-side JavaScript	TCP (TLS)	Ricezione delle connessioni dal browser a Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. È possibile modificare il numero di porta predefinito durante l'installazione di Kaspersky Security Center Web Console. Se si installa Kaspersky Security Center Web Console nel sistema operativo Linux ALT, è necessario specificare un numero di porta diverso da 8080, poiché la porta 8080 è utilizzata dal sistema operativo.

La tabella seguente mostra la porta utilizzata dai dispositivi gestiti in cui è installato Network Agent.

Porte utilizzate da Network Agent

Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta	Ambito
15000	klnagent	UDP	Segnali di gestione da Administration Server o dal punto di distribuzione ai Network Agent	Gestione dei dispositivi client. È possibile modificare il numero di porta predefinito nelle impostazioni del criterio di Network Agent.
15000	klnagent	Trasmissione UDP	Ottenimento dei dati su altri Network Agent all'interno dello stesso dominio di trasmissione (i dati vengono quindi inviati ad Administration Server)	Distribuzione degli aggiornamenti e dei pacchetti di installazione.
15001	klnagent	UDP	Ricezione di richieste multicast da un punto di distribuzione (se in uso)	Ricezione di aggiornamenti e pacchetti di installazione da un punto di distribuzione. È possibile modificare il numero di porta predefinito nella finestra delle proprietà del punto di distribuzione.
30522, 30523 (porte sull'interfaccia localhost)	klnagent	TCP	Ricezione degli aggiornamenti delle applicazioni Kaspersky da Administration Server tramite il componente FileTransferBridge	Dispositivi gestiti che ricevono gli aggiornamenti delle applicazioni Kaspersky dall'Administration Server specificato come sorgente degli aggiornamenti del database.

Si noti che il processo klnagent può anche richiedere porte libere dall'intervallo di porte dinamiche del sistema operativo di un endpoint. Queste porte vengono assegnate automaticamente al processo klnagent dal sistema operativo, quindi il processo klnagent può utilizzare alcune porte usate da un altro software. Se il processo klnagent influisce sulle operazioni del software, modificare le impostazioni delle porte in questo software o modificare l'intervallo di porte dinamiche predefinito nel sistema operativo per escludere la porta utilizzata dal software interessato.

Tenere inoltre presente che i suggerimenti sulla compatibilità di Kaspersky Security Center Linux con il software di terzi sono descritti solo come riferimento e potrebbero non essere applicabili alle nuove versioni del software di terzi. I suggerimenti descritti per la configurazione delle porte si basano sull'esperienza dell'Assistenza tecnica e sulle nostre best practice.

La tabella seguente mostra le porte utilizzato da un dispositivo gestito in cui è installato Network Agent con il ruolo di punto di distribuzione. Oltre alle porte utilizzate dai Network Agent, anche le porte elencate sono utilizzate dai dispositivi del punto di distribuzione (vedere la tabella sopra).

Porte utilizzate da Network Agent con il ruolo di punto di distribuzione

Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta	Ambito
13000	klnagent	TCP (TLS)	Ricezione di connessioni da Network Agent e gateway di connessione	Gestione dei dispositivi client, distribuzione degli aggiornamenti e dei pacchetti di installazione. È possibile modificare il numero di porta predefinito nelle proprietà del punto di distribuzione.
13111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	ksnproxy	TCP	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN. È possibile modificare il numero di porta predefinito nelle proprietà del punto di distribuzione.
15111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	ksnproxy	UDP	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN. È possibile modificare il numero di porta predefinito nelle proprietà del punto di distribuzione.

La tabella seguente mostra le porte utilizzate da un dispositivo controller di dominio.

Porte utilizzate da un dispositivo controller di dominio

Numero di porta	Protocollo	Ambito della porta	Ambito
389	LDAP su TCP o UDP	Connessione a un server LDAP	Polling del controller di dominio
636	LDAP su TLS	Connessione a un server LDAP	Polling del controller di dominio

Porte utilizzate da Kaspersky Security Center Web Console

La tabella seguente elenca le porte che devono essere aperte nel dispositivo in cui è installato Kaspersky Security Center Web Console Server (noto anche come Kaspersky Security Center Web Console).

Porte utilizzate da Kaspersky Security Center Web Console

Numero di porta	Nome servizio	Protocollo	Ambito della porta	Ambito
2001	Kaspersky Security Center Product Plugins Server	HTTPS	Porta API utilizzata dai processi del plug-in di gestione per ricevere richieste da "Kaspersky Security Center Web Console Management Service"	Esecuzione dei processi di nodi dei plug-in di gestione
1329, 2003	Kaspersky Security Center Web Console Management Service	HTTPS	Porte API utilizzate per ricevere richieste da "Kaspersky Security Center Web Console Management Service" in esecuzione nello stesso dispositivo	Aggiornamento dei componenti di Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	Porta API utilizzata per ricevere richieste da "Kaspersky Security Center Web Console Management Service" in esecuzione nello stesso dispositivo	Esecuzione dei processi di nodi di Kaspersky Security Center Web Console
8200	—	HTTP	Porta API utilizzata per generare certificati tramite HashiCorp Vault (per maggiori dettagli, consultare il sito Web di HashiCorp Vault)	Installazione di Kaspersky Security Center Web Console e aggiornamento dei componenti di Kaspersky Security Center Web Console
4150, 4151, 4152	Kaspersky Security Center Web Console Message Queue	HTTPS	Porte API del broker di messaggi utilizzate per la comunicazione tra i processi di Kaspersky	Interazione tra Kaspersky Security Center Web Console e plug-in di gestione

			Security Center Web Console e dei plug-in di gestione	

Concetti di base

In questa sezione sono illustrati i concetti di base relativi a Kaspersky Security Center Linux.

Administration Server

I componenti di Kaspersky Security Center consentono la gestione remota delle applicazioni Kaspersky installate nei dispositivi client.

I dispositivi in cui è installato il componente Administration Server sono denominati *Administration Server* (o semplicemente *server*). Gli Administration Server devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Administration Server viene installato nei dispositivi come un servizio con il seguente set di attributi:

- Con il nome `kladminserver_srv`
- Impostato per l'avvio automatico all'avvio del sistema operativo
- Con l'account `ksc` o l'account utente selezionato durante l'installazione di Administration Server

Fare riferimento al seguente argomento per l'elenco completo delle impostazioni di installazione: Installazione di Kaspersky Security Center Linux.

Administration Server esegue le seguenti funzioni:

- Memorizzazione della struttura dei gruppi di amministrazione
- Archiviazione di informazioni sulla configurazione dei dispositivi client
- Organizzazione degli archivi per i pacchetti di distribuzione dell'applicazione
- Installazione remota delle applicazioni nei dispositivi client e rimozione delle applicazioni
- Aggiornamento dei database e dei moduli software delle applicazioni Kaspersky
- Gestione di criteri e attività nei dispositivi client
- Archiviazione di informazioni sugli eventi che si sono verificati nei dispositivi client
- Generazione di rapporti sull'esecuzione delle applicazioni Kaspersky
- Distribuzione delle chiavi di licenza ai dispositivi client e archiviazione delle informazioni sulle chiavi di licenza
- Invio di notifiche sullo stato di avanzamento delle attività (ad esempio, il rilevamento di virus in un dispositivo client)

Denominazione degli Administration Server nell'interfaccia dell'applicazione

Nell'interfaccia di Kaspersky Security Center Web Console, gli Administration Server possono avere i seguenti nomi:

- Nome del dispositivo Administration Server, ad esempio: "*nome_dispositivo*" o "Administration Server: *nome_dispositivo*".
- Indirizzo IP del dispositivo Administration Server, ad esempio: "*Indirizzo_IP*" o "Administration Server: *Indirizzo_IP*".
- Gli Administration Server secondari e gli Administration Server virtuali hanno nomi personalizzati da specificare quando si connette un Administration Server virtuale o secondario all'Administration Server primario.
- Se si utilizza Kaspersky Security Center Web Console installata in un dispositivo Linux, l'applicazione visualizza i nomi degli Administration Server specificati come attendibili nel file di risposta.

È possibile connettersi ad Administration Server tramite Kaspersky Security Center Web Console.

Gerarchia di Administration Server

Gli Administration Server possono essere organizzati in una gerarchia. Ogni Administration Server può disporre di diversi Administration Server secondari (denominati *server secondari*) a diversi livelli di nidificazione della gerarchia. Non vi sono limiti per il livello di nidificazione dei server secondari. I gruppi di amministrazione dell'Administration Server primario includeranno i dispositivi client di tutti gli Administration Server secondari. In tal modo, è possibile gestire sezioni isolate e indipendenti di reti tramite differenti Administration Server che vengono a loro volta gestiti dal server primario.

In una gerarchia, un Administration Server basato su Linux può fungere sia da server primario che da server secondario. Il server primario basato su Linux può gestire sia i server secondari basati su Linux che quelli basati su Windows. Un server primario basato su Windows può gestire un server secondario basato su Linux.

Gli *Administration Server virtuali* sono casi particolari di Administration Server secondari.

La gerarchia degli Administration Server può essere utilizzata per le seguenti operazioni:

- Ridurre il carico su Administration Server (rispetto all'utilizzo di un singolo Administration Server installato per un'intera rete).
- Ridurre il traffico nella rete Intranet e semplificare il lavoro con le filiali remote. Non è necessario stabilire connessioni tra l'Administration Server primario e tutti i dispositivi della rete, che possono ad esempio essere collocati in altre aree geografiche. È sufficiente installare un Administration Server secondario in ogni segmento della rete, distribuire i dispositivi tra i gruppi di amministrazione dei server secondari e stabilire connessioni tra i server secondari e il server primario tramite canali di comunicazione ad alta velocità.
- Distribuire le responsabilità tra gli amministratori della protezione anti-virus. Tutte le capacità di monitoraggio e gestione centralizzati dello stato della protezione anti-virus nelle reti aziendali rimangono disponibili.
- Utilizzare Kaspersky Security Center dai provider di servizi. Un provider di servizi deve installare soltanto Kaspersky Security Center e Kaspersky Security Center Web Console. Per gestire numerosi dispositivi client di varie organizzazioni, un provider di servizi può aggiungere Administration Server secondari (inclusi i server virtuali) a una gerarchia di Administration Server.

Ogni dispositivo incluso nella gerarchia dei gruppi di amministrazione può essere connesso a un unico Administration Server. È necessario monitorare in modo indipendente la connessione dei dispositivi agli Administration Server. Utilizzare la funzionalità per la ricerca di dispositivi nei gruppi di amministrazione di differenti server in base agli attributi di rete.

Administration Server virtuale

Un Administration Server virtuale (denominato anche *server virtuale*) è un componente di Kaspersky Security Center Linux progettato per la gestione della protezione anti-virus della rete di un'organizzazione client.

Un Administration Server virtuale è un particolare tipo di Administration Server secondario e presenta le seguenti limitazioni rispetto a un Administration Server fisico:

- Un Administration Server virtuale può essere creato solo in un Administration Server primario.
- L'Administration Server virtuale utilizza il database dell'Administration Server primario durante il relativo funzionamento. Le attività di backup e ripristino dei dati, nonché le attività di scansione e download degli aggiornamenti, non sono supportate in un Administration Server virtuale.
- Un server virtuale non supporta la creazione di Administration Server secondari (inclusi server virtuali).

L'Administration Server virtuale presenta inoltre le seguenti restrizioni:

- Nella finestra delle proprietà di Administration Server virtuale il numero delle sezioni è limitato.
- Per eseguire l'installazione delle applicazioni Kaspersky in remoto nei dispositivi client gestiti dall'Administration Server virtuale, è necessario verificare che Network Agent sia installato in uno dei dispositivi client per assicurare la comunicazione con l'Administration Server virtuale. Alla prima connessione con l'Administration Server virtuale, il dispositivo verrà automaticamente designato come punto di distribuzione e opererà come un gateway di connessione tra i dispositivi client e l'Administration Server virtuale.
- Un server virtuale può eseguire il polling della rete solo tramite i punti di distribuzione.
- Per riavviare un server virtuale che presenta un malfunzionamento, Kaspersky Security Center Linux riavvia l'Administration Server primario e tutti gli Administration Server virtuali.
- Agli utenti creati in un server virtuale non può essere assegnato un ruolo in Administration Server.

L'amministratore di un Administration Server virtuale dispone di tutti i privilegi per lo specifico server virtuale.

Server Web

Il *server Web* di Kaspersky Security Center (di seguito denominato anche *server Web*) è un componente di Kaspersky Security Center installato insieme ad Administration Server. Il server Web è progettato per la trasmissione tramite una rete di pacchetti di installazione indipendenti e file da una cartella condivisa.

Quando si crea un pacchetto di installazione indipendente, questo viene automaticamente pubblicato nel server Web. Il collegamento per il download del pacchetto indipendente viene visualizzato nell'elenco dei pacchetti di installazione indipendenti creati. Se necessario, è possibile annullare la pubblicazione del pacchetto indipendente o pubblicarlo nuovamente sul server Web.

La cartella condivisa è progettata come un'area di archiviazione per le informazioni disponibile per tutti gli utenti dei dispositivi gestiti tramite Administration Server. Se un utente non ha accesso diretto alla cartella condivisa, è possibile fornirgli le informazioni contenute nella cartella utilizzando il server Web.

Per fornire agli utenti le informazioni nella cartella condivisa utilizzando il server Web, l'amministratore deve creare una sottocartella denominata public nella cartella condivisa e incollare le informazioni in tale sottocartella.

La sintassi del collegamento per il trasferimento delle informazioni è la seguente:

`https://<nome server Web>:<porta HTTPS>/public/<oggetto>`

dove:

- `<nome server Web>` è il nome del server Web di Kaspersky Security Center.
- `<porta HTTPS>` è una porta HTTPS del server Web definita dall'amministratore. La porta HTTPS può essere impostata nella sezione **Server Web** della finestra delle proprietà di Administration Server. Il numero di porta predefinito è 8061.
- `<oggetto>` è la sottocartella o il file reso accessibile all'utente.

L'amministratore può inviare il nuovo collegamento all'utente con qualsiasi sistema (ad esempio, tramite e-mail).

Utilizzando questo collegamento, l'utente può scaricare le informazioni richieste in un dispositivo locale.

Network Agent

L'interazione tra Administration Server e i dispositivi viene eseguita dal componente *Network Agent* di Kaspersky Security Center Linux. Network Agent deve essere installato in tutti i dispositivi in cui viene utilizzato Kaspersky Security Center Linux per gestire applicazioni Kaspersky.

Un dispositivo con Network Agent installato è denominato *dispositivo gestito* o *dispositivo*. È possibile scaricare il pacchetto di installazione per Network Agent dalle seguenti risorse:

- Archivio di Administration Server (è necessario avere installato Administration Server)
- Sito Web di Kaspersky

Network Agent for Linux viene installato nei dispositivi come un servizio con il seguente set di attributi:

- Il nome "Kaspersky Network Agent"
- Impostato per l'avvio automatico all'avvio del sistema operativo
- Utilizzo dell'account root

Network Agent for Windows viene installato nei dispositivi come un servizio con il seguente set di attributi:

- Il nome "Kaspersky Security Center Network Agent"

- Impostato per l'avvio automatico all'avvio del sistema operativo
- Utilizzo dell'account LocalSystem

I nomi dei processi di servizio:

- Per Linux:
  - klnagent64.service (per un sistema operativo a 64 bit)
  - klnagent.service (per un sistema operativo a 32 bit)
- Per Windows:
  - klnagent

Per impostazione predefinita, Network Agent è installato nei seguenti percorsi:

- Per Linux:
  - Sistemi a 32 bit: /opt/kaspersky/klnagent/
  - Sistemi a 64 bit: /opt/kaspersky/klnagent64/
- Per Windows:
  - Sistemi a 32 bit: C:\Program Files\Kaspersky Lab\NetworkAgent
  - Sistemi a 64 bit: C:\Program Files (x86)\Kaspersky Lab\NetworkAgent

Per i dispositivi Windows è possibile specificare una cartella diversa per l'installazione di Network Agent nelle impostazioni del pacchetto di installazione. Tuttavia, per i dispositivi Linux, Network Agent può essere installato solo nella directory predefinita.

La cartella di installazione di Network Agent contiene anche utilità per la gestione e la diagnosi del funzionamento di Network Agent, come le utilità klmover e klnagchk.

Quando si installa Administration Server, la versione server di Network Agent viene installata automaticamente insieme ad Administration Server. Tuttavia, per gestire il dispositivo Administration Server come qualsiasi altro dispositivo gestito, installare Network Agent for Linux nel dispositivo Administration Server. In questo caso, Network Agent per Linux è installato e funziona indipendentemente dalla versione server di Network Agent installata insieme ad Administration Server.

Network Agent sincronizza il dispositivo gestito con Administration Server. È consigliabile impostare l'intervallo di sincronizzazione (anche denominato *heartbeat*) su 15 minuti per 10.000 dispositivi gestiti.

Gruppi di amministrazione

Un *gruppo di amministrazione* (di seguito denominato anche *gruppo*) è un set logico di dispositivi gestiti combinati in base a una specifica caratteristica allo scopo di gestire i dispositivi raggruppati come una singola unità in Kaspersky Security Center Linux.

Tutti i dispositivi gestiti all'interno di un gruppo di amministrazione sono configurati in modo da eseguire quanto segue:

- Utilizzare le stesse impostazioni dell'applicazione (che possono essere specificate nei criteri di gruppo).
- Utilizzare una modalità operativa comune per tutte le applicazioni grazie alla creazione di attività di gruppo con impostazioni specificate. Tramite le attività di gruppo è ad esempio possibile creare e installare un pacchetto di installazione comune, aggiornare i database e i moduli dell'applicazione, eseguire la scansione del dispositivo su richiesta e abilitare la protezione in tempo reale.

Un dispositivo gestito può appartenere a un solo gruppo di amministrazione.

È possibile creare gerarchie con qualsiasi livello di nidificazione per gli Administration Server e i gruppi. Un singolo livello della gerarchia può comprendere Administration Server secondari e virtuali, gruppi e dispositivi gestiti. È possibile spostare i dispositivi da un gruppo all'altro senza spostarli fisicamente. Ad esempio, se la posizione di un dipendente all'interno dell'azienda cambia da addetto alla contabilità a sviluppatore, è possibile spostare il dispositivo del dipendente dal gruppo di amministrazione Contabilità al gruppo di amministrazione Sviluppatori. Il dispositivo riceverà automaticamente le impostazioni dell'applicazione necessarie per gli sviluppatori.

Dispositivo gestito

Un *dispositivo gestito* è un dispositivo in cui viene eseguito Linux, Windows o macOS e in cui è installato Network Agent. È possibile gestire tali dispositivi creando attività e criteri per le applicazioni installate nei dispositivi. È inoltre possibile ricevere rapporti dai dispositivi gestiti.

È possibile designare un dispositivo gestito come punto di distribuzione e come gateway di connessione.

Un dispositivo può essere gestito da un solo Administration Server. Un unico Administration Server può gestire fino a 20.000 dispositivi.

Dispositivo non assegnato

Un *dispositivo non assegnato* è un dispositivo della rete che non è stato incluso in alcun gruppo di amministrazione. È possibile eseguire alcune azioni sui dispositivi non assegnati, ad esempio spostarli nei gruppi di amministrazione o installarvi applicazioni.

Quando viene individuato un nuovo dispositivo nella rete, questo dispositivo viene inserito nel gruppo di amministrazione **Dispositivi non assegnati**. È possibile configurare regole per lo spostamento automatico dei dispositivi in altri gruppi di amministrazione dopo il rilevamento.

Workstation dell'amministratore

I dispositivi in cui è installato Kaspersky Security Center Web Console Server sono denominati *workstation dell'amministratore*. Gli amministratori possono utilizzare tali dispositivi per la gestione remota centralizzata delle applicazioni Kaspersky installate nei dispositivi client.

Non vi sono limitazioni per il numero di workstation dell'amministratore. Da qualsiasi workstation dell'amministratore è possibile gestire contemporaneamente i gruppi di amministrazione di diversi Administration Server in rete. Una workstation dell'amministratore può essere connessa a un Administration Server (fisico o virtuale) a qualsiasi livello di gerarchia.

È possibile includere una workstation dell'amministratore in un gruppo di amministrazione come dispositivo client.

All'interno dei gruppi di amministrazione di qualsiasi Administration Server, lo stesso dispositivo può operare come un client di Administration Server, un Administration Server o una workstation dell'amministratore.

Plug-in Web di gestione

Un componente speciale (il *plug-in Web di gestione*) viene utilizzato per l'amministrazione remota del software Kaspersky tramite Kaspersky Security Center Web Console. Da questo momento il plug-in Web di gestione verrà denominato anche *plug-in di gestione*. Il plug-in di gestione è un'interfaccia tra Kaspersky Security Center Web Console e un'applicazione Kaspersky specifica. Con un plug-in di gestione è possibile configurare le attività e i criteri per l'applicazione.

È possibile scaricare i plug-in Web di gestione dalla pagina Web del Servizio di assistenza tecnica di Kaspersky.

Il plug-in di gestione offre i seguenti elementi:

- Interfaccia per la creazione e la modifica di impostazioni e attività delle applicazioni
- Interfaccia per la creazione e la modifica di criteri e profili criterio per la configurazione centralizzata e remota dei dispositivi e delle applicazioni Kaspersky
- Trasmissione di eventi generati dall'applicazione
- Kaspersky Security Center Web Console consente di visualizzare eventi e dati relativi al funzionamento dell'applicazione e le statistiche trasmesse dai dispositivi client

Criteri

Un *criterio* è un set di impostazioni dell'applicazione Kaspersky che vengono applicate a un gruppo di amministrazione e ai relativi sottogruppi. È possibile installare diverse applicazioni Kaspersky nei dispositivi di un gruppo di amministrazione. Kaspersky Security Center fornisce un singolo criterio per ogni applicazione Kaspersky in un gruppo di amministrazione. Un criterio può avere uno dei seguenti stati:

Lo stato del criterio

Stato	Descrizione
Attivo	Il criterio corrente applicato al dispositivo. Può essere attivo un solo criterio per un'applicazione Kaspersky in ogni gruppo di amministrazione. I dispositivi applicano i valori delle impostazioni di un criterio attivo per un'applicazione Kaspersky.
Inattivo	Un criterio che non è attualmente applicato a un dispositivo.
Fuori sede	Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.

I criteri funzionano secondo le seguenti regole:

- È possibile configurare diversi criteri con differenti impostazioni per una singola applicazione.
- Un solo criterio può essere attivo per l'applicazione corrente.
- Un criterio può avere criteri secondari.

In generale è possibile utilizzare i criteri in preparazione a situazioni di emergenza, come un attacco virus. Ad esempio in caso di attacco tramite unità flash, è possibile attivare un criterio che blocca l'accesso alle unità flash. In questo caso il criterio attivo corrente diventa automaticamente inattivo.

Per evitare di dover gestire più criteri, ad esempio quando diverse occasioni presuppongono solo la modifica di più impostazioni, è possibile utilizzare i profili criterio.

Un *profilo criterio* è un sottoinsieme denominato di valori delle impostazioni dei criteri che sostituisce i valori delle impostazioni di un criterio. Un profilo criterio influisce sulla creazione delle impostazioni ottimizzate in un dispositivo gestito. Per *impostazioni effettive* si intende un insieme di impostazioni dei criteri, impostazioni dei profili criterio e impostazioni delle applicazioni locali attualmente applicate nel dispositivo.

I profili criterio funzionano secondo le seguenti regole:

- Un profilo criterio assume validità quando si verifica una condizione di attivazione specifica.
- I profili criterio contengono valori delle impostazioni che differiscono dalle impostazioni dei criteri.
- L'attivazione di un profilo criterio modifica le impostazioni effettive del dispositivo gestito.
- Un criterio può includere al massimo 100 profili criterio.

Profili criterio

Talvolta può essere necessario creare più istanze di un singolo criterio per diversi gruppi di amministrazione; è inoltre possibile modificare le impostazioni di questi criteri in modo centralizzato. Le istanze potrebbero avere solo una o due impostazioni differenti. Ad esempio, a tutti gli addetti alla contabilità di un'azienda viene applicato lo stesso criterio, ma quelli di livello senior possono utilizzare unità flash, a differenza degli altri. In questo caso, l'applicazione dei criteri ai dispositivi solo tramite la gerarchia dei gruppi di amministrazione può essere poco pratica.

Per evitare di creare più istanze di un singolo criterio, Kaspersky Security Center Linux consente di creare *profili criterio*. I profili criterio sono necessari per consentire l'esecuzione dei dispositivi all'interno di un unico gruppo di amministrazione con diverse impostazioni del criterio.

Un profilo criterio è un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita *condizione di attivazione del profilo*. I profili contengono solo le impostazioni diverse dal criterio "di base" che è attivo nel dispositivo gestito. L'attivazione di un profilo modifica le impostazioni del criterio "di base" che erano inizialmente attive nel dispositivo. Le impostazioni modificate assumono i valori specificati nel profilo.

Attività

Kaspersky Security Center Linux consente di gestire le applicazioni di protezione Kaspersky installate nei dispositivi creando ed eseguendo *attività*. Le attività sono necessarie per l'installazione, l'avvio e l'arresto delle applicazioni, la scansione dei file, l'aggiornamento dei database e dei moduli software, oltre che per eseguire altre azioni sulle applicazioni.

Le attività per un'applicazione specifica possono essere create solo se è installato il plug-in di gestione per tale applicazione.

Le attività possono essere eseguite nell'Administration Server e nei dispositivi.

Le seguenti attività vengono eseguite nell'Administration Server:

- Distribuzione automatica dei rapporti
- Download degli aggiornamenti nell'archivio di Administration Server
- Backup dei dati di Administration Server
- Manutenzione del database

I seguenti tipi di attività vengono eseguiti nei dispositivi:

- *Attività locali* - Attività eseguite in un dispositivo specifico

  Le attività locali possono essere modificate dall'amministratore utilizzando Kaspersky Security Center Web Console oppure dall'utente di un dispositivo remoto (ad esempio attraverso l'interfaccia dell'applicazione di protezione). Se un'attività locale viene modificata contemporaneamente dall'amministratore e dall'utente di un dispositivo gestito, hanno effetto le modifiche apportate dall'amministratore perché hanno una priorità più alta.

- *Attività di gruppo* - Attività eseguite su tutti i dispositivi di un gruppo specifico

  A meno che non sia diversamente specificato nelle proprietà dell'attività, un'attività di gruppo si applica anche a tutti i sottogruppi del gruppo selezionato. Un'attività di gruppo influisce anche (facoltativamente) sui dispositivi connessi agli Administration Server secondari e virtuali distribuiti nel gruppo o in uno dei relativi sottogruppi.

- *Attività globali* - Attività eseguite su un set di dispositivi, indipendentemente dalla loro appartenenza a un gruppo

Per ogni applicazione è possibile creare attività di gruppo, attività globali o attività locali.

È possibile apportare modifiche alle impostazioni delle attività, visualizzarne l'avanzamento, copiarle, esportarle, importarle ed eliminarle.

Le attività vengono avviate in un dispositivo solo se l'applicazione per cui l'attività è stata creata è in esecuzione.

I risultati delle attività sono salvati nel registro eventi Syslog e nel registro eventi di Kaspersky Security Center Linux, sia in modo centralizzato in Administration Server che localmente in ogni dispositivo.

Non includere dati privati nelle impostazioni dell'attività. Ad esempio, non specificare la password dell'amministratore del dominio.

Ambito attività

L'*ambito di un'attività* è il set di dispositivi in cui viene eseguita l'attività. I tipi di ambito sono i seguenti:

- Per un'*attività locale*, l'ambito è il dispositivo stesso.
- Per un'*attività di Administration Server*, l'ambito è Administration Server.

- Per un'*attività di gruppo*, l'ambito è l'elenco dei dispositivi inclusi nel gruppo.

Durante la creazione di un'*attività globale*, è possibile utilizzare i seguenti metodi per specificare l'ambito:

- Specificare manualmente specifici dispositivi.

  È possibile utilizzare un indirizzo IP (o un intervallo IP) o un nome DNS come indirizzo del dispositivo.

- Importare un elenco di dispositivi da un file .txt con gli indirizzi dei dispositivi da aggiungere (ogni indirizzo deve essere specificato su una riga distinta).

  Se si importa un elenco di dispositivi da un file o se ne crea uno manualmente e i dispositivi vengono identificati con i rispettivi nomi, l'elenco deve contenere solo dispositivi per cui sono già state immesse le informazioni nel database di Administration Server. Inoltre, le informazioni devono essere state immesse al momento della connessione dei dispositivi o durante la device discovery.

- Specificare una selezione dispositivi.

  Nel corso del tempo, l'ambito un'attività si modifica, perché il set di dispositivi inclusi nella selezione cambia. Una selezione di dispositivi può essere creata sulla base degli attributi dei dispositivi, incluso il software installato in un dispositivo, e utilizzando i tag assegnati ai dispositivi. Una selezione dispositivi è il modo più flessibile per specificare l'ambito di un'attività.

  Le attività per le selezioni dispositivi vengono sempre eseguite in base a una pianificazione da Administration Server. Queste attività non possono essere eseguite nei dispositivi che non dispongono di una connessione ad Administration Server. Le attività il cui ambito è specificato tramite altri metodi vengono eseguite direttamente nei dispositivi, pertanto non dipendono dalla connessione del dispositivo ad Administration Server.

  Le attività per le selezioni dispositivi non vengono eseguite in base all'ora locale di un dispositivo, ma in base all'ora locale di Administration Server. Le attività il cui ambito è specificato tramite altri metodi vengono eseguite in base all'ora locale di un dispositivo.

Relazioni tra impostazioni locali delle applicazioni e criteri

È possibile utilizzare i criteri per impostare valori identici delle impostazioni delle applicazioni per tutti i dispositivi nel gruppo.

I valori delle impostazioni specificati da un criterio possono essere ridefiniti per singoli dispositivi in un gruppo utilizzando le impostazioni locali delle applicazioni. È possibile impostare soltanto i valori delle impostazioni che il criterio consente di modificare, ovvero le impostazioni sbloccate.

Il valore di un'impostazione utilizzata da un'applicazione in un dispositivo client è determinato dalla posizione del lucchetto (🔒) per l'impostazione nel criterio:

- Se la modifica di un'impostazione è bloccata, viene utilizzato lo stesso valore definito nel criterio in tutti i dispositivi client.

- Se la modifica di un'impostazione è "sbloccata", l'applicazione utilizza in ogni dispositivo client il valore dell'impostazione locale invece di quello specificato nel criterio. Il valore del parametro può quindi essere modificato nelle impostazioni locali dell'applicazione.

In questo modo, quando l'attività viene eseguita in un dispositivo client, l'applicazione utilizza impostazioni definite in due modi diversi:

- tramite le impostazioni delle attività e le impostazioni locali delle applicazioni, se la modifica dell'impostazione nel criterio non è bloccata.

- tramite il criterio di gruppo, se la modifica dell'impostazione è bloccata.

Le impostazioni locali delle applicazioni vengono modificate dopo la prima applicazione del criterio in base alle relative impostazioni.

Punto di distribuzione

Per *punto di distribuzione* (prima noto come Update Agent) si intende un dispositivo in cui è installato Network Agent, utilizzato per la distribuzione degli aggiornamenti, l'installazione remota delle applicazioni e il recupero di informazioni sui dispositivi della rete.

Le funzionalità e i casi d'uso di Network Agent installato su un dispositivo utilizzato come punto di distribuzione variano a seconda del sistema operativo.

Un punto di distribuzione può eseguire le seguenti funzioni:

- Distribuire gli aggiornamenti e i pacchetti di installazione ricevuti da Administration Server ai dispositivi client nel gruppo (inclusa la distribuzione mediante il multicasting tramite UDP). Gli aggiornamenti possono essere ricevuti da Administration Server o dai server di aggiornamento Kaspersky. Nel secondo caso è necessario creare un'attività di aggiornamento per il punto di distribuzione.

  I punti di distribuzione accelerano la distribuzione degli aggiornamenti e riducono l'utilizzo di risorse di Administration Server.

- Distribuire criteri e attività di gruppo attraverso il multicasting tramite UDP.

- Operare come gateway per la connessione all'Administration Server per i dispositivi di un gruppo di amministrazione.

  Se è impossibile stabilire una connessione diretta tra i dispositivi gestiti nel gruppo e Administration Server, il punto di distribuzione può essere utilizzato come gateway di connessione ad Administration Server per il gruppo. In questo caso, i dispositivi gestiti sono connessi al gateway di connessione, che a sua volta è connesso ad Administration Server.

  La presenza di un punto di distribuzione che opera come gateway di connessione non esclude la possibilità di una connessione diretta tra i dispositivi gestiti e Administration Server. Se il gateway di connessione non è disponibile, ma è tecnicamente possibile la connessione diretta ad Administration Server, i dispositivi gestiti vengono connessi direttamente ad Administration Server.

- Eseguire il polling della rete per rilevare nuovi dispositivi e aggiornare le informazioni sui dispositivi esistenti. Un punto di distribuzione può applicare gli stessi metodi di device discovery di Administration Server.

- Eseguire l'installazione remota delle applicazioni Kaspersky e di altri fornitori di software, inclusa l'installazione in dispositivi client senza Network Agent.

  Questa funzionalità consente di trasferire in remoto i pacchetti di installazione di Network Agent ai dispositivi client disponibili nelle reti a cui l'Administration Server non ha accesso diretto.

- Fungere da server proxy che partecipa a Kaspersky Security Network (KSN).

  È possibile abilitare il proxy KSN da parte del punto di distribuzione per fare in modo che il dispositivo abbia il ruolo di Proxy KSN. In questo caso, il servizio proxy KSN viene eseguito nel dispositivo.

I file vengono trasmessi da Administration Server a un punto di distribuzione tramite HTTP o, se la connessione SSL è abilitata, HTTPS. L'utilizzo di HTTP o HTTPS garantisce un livello di prestazioni superiore rispetto a SOAP, grazie alla riduzione del traffico.

Ai dispositivi in cui è installato Network Agent può essere assegnato il ruolo di punti di distribuzione manualmente (dall'amministratore) o automaticamente (dall'Administration Server). L'elenco completo dei punti di distribuzione per i gruppi di amministrazione specificati è visualizzato nel rapporto sull'elenco dei punti di distribuzione.

L'ambito di un punto di distribuzione è il gruppo di amministrazione a cui è stato assegnato dall'amministratore, nonché i relativi sottogruppi a tutti i livelli. Se sono stati assegnati più punti di distribuzione nella gerarchia dei gruppi di amministrazione, Network Agent nel dispositivo gestito si connette al punto di distribuzione più vicino nella gerarchia.

Se i punti di distribuzione sono assegnati automaticamente da Administration Server, vengono assegnati in base ai domini di trasmissione anziché in base ai gruppi di amministrazione. Questo si verifica quando tutti i domini di trasmissione sono noti. Network Agent scambia messaggi con altri Network Agent nella stessa subnet e invia ad Administration Server informazioni su se stesso e su altri Network Agent. Administration Server può utilizzare tali informazioni per raggruppare i Network Agent in base ai domini di trasmissione. I domini di trasmissione diventano noti ad Administration Server in seguito al polling di oltre il 70% dei Network Agent nei gruppi di amministrazione. Administration Server esegue il polling dei domini di trasmissione ogni due ore. In seguito all'assegnazione in base ai domini di trasmissione, i punti di distribuzione non possono essere riassegnati in base ai gruppi di amministrazione.

Se l'amministratore assegna manualmente i punti di distribuzione, questi possono essere assegnati a gruppi di amministrazione o posizioni di rete.

I Network Agent con un profilo di connessione attivo non partecipano al rilevamento dei domini di trasmissione.

Kaspersky Security Center Linux assegna a ciascun Network Agent un indirizzo IP multicast univoco diverso da tutti gli altri indirizzi. Questo consente di evitare il sovraccarico della rete che potrebbe verificarsi a causa di sovrapposizioni IP. Gli indirizzi IP multicast assegnati nelle versioni precedenti dell'applicazione non verranno modificati.

Se due o più punti di distribuzione vengono assegnati in un'unica area di rete o in un singolo gruppo di amministrazione, uno di loro diventa il punto di distribuzione attivo, mentre gli altri diventano punti di distribuzione standby. Il punto di distribuzione attivo scarica gli aggiornamenti e i pacchetti di installazione direttamente da Administration Server, mentre i punti di distribuzione standby ricevono gli aggiornamenti solo dal punto di distribuzione attivo. In questo caso, i file vengono scaricati una sola volta da Administration Server e in seguito distribuiti tra i punti di distribuzione. Se il punto di distribuzione attivo diventa non disponibile per qualsiasi motivo, uno dei punti di distribuzione standby diventa attivo. Administration Server assegna automaticamente a un punto di distribuzione il ruolo di standby.

Lo stato di un punto di distribuzione (*Attivo* / *Standby*) è visualizzato con una casella di controllo nel rapporto di klnagchk.

Un punto di distribuzione richiede almeno 4 GB di spazio disponibile sul disco. Se lo spazio disponibile sul disco del punto di distribuzione è inferiore a 2 GB, Kaspersky Security Center Linux crea un problema di sicurezza con il livello di importanza *Avviso*. Il problema di sicurezza sarà pubblicato nelle proprietà del dispositivo, nella sezione **Problemi di sicurezza**.

L'esecuzione delle attività di installazione remota in un dispositivo assegnato come punto di distribuzione richiede ulteriore spazio libero su disco. Il volume di spazio disponibile sul disco deve essere superiore alle dimensioni totali di tutti i pacchetti di installazione da installare.

L'esecuzione di attività di aggiornamento (installazione delle patch) e di correzione vulnerabilità in un dispositivo con il ruolo di punto di distribuzione richiede ulteriore spazio libero su disco. Il volume di spazio disponibile sul disco deve essere almeno il doppio rispetto alle dimensioni totali di tutte le patch da installare.

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Gateway di connessione

Un *gateway di connessione* è un Network Agent che funziona in modalità speciale. Un gateway di connessione accetta le connessioni da altri Network Agent e le trasmette ad Administration Server tramite la propria connessione con il server. A differenza di un normale Network Agent, un gateway di connessione attende le connessioni da Administration Server anziché stabilire connessioni ad Administration Server.

Un gateway di connessione può ricevere connessioni da un massimo di 10.000 dispositivi.

Sono disponibili due opzioni per utilizzare i gateway di connessione:

- È consigliabile installare un gateway di connessione in una rete perimetrale. Per altri Network Agent installati in dispositivi fuori sede è necessario configurare appositamente una connessione ad Administration Server tramite il gateway di connessione.

  Un gateway di connessione non modifica o elabora in alcun modo i dati trasmessi dai Network Agent ad Administration Server. Inoltre, non scrive questi dati in alcun buffer e non può quindi accettare dati da un Network Agent e in seguito inoltrarli ad Administration Server. Se Network Agent tenta di connettersi ad Administration Server tramite il gateway di connessione, ma il gateway di connessione non riesce a connettersi ad Administration Server, Network Agent percepisce Administration Server come inaccessibile. Tutti i dati rimangono in Network Agent (non nel gateway di connessione).

  Un gateway di connessione non può connettersi ad Administration Server tramite un altro gateway di connessione. Network Agent non può quindi essere contemporaneamente un gateway di connessione e utilizzare un gateway di connessione per connettersi ad Administration Server.

  Tutti i gateway di connessione sono inclusi nell'elenco dei punti di distribuzione nelle proprietà di Administration Server.

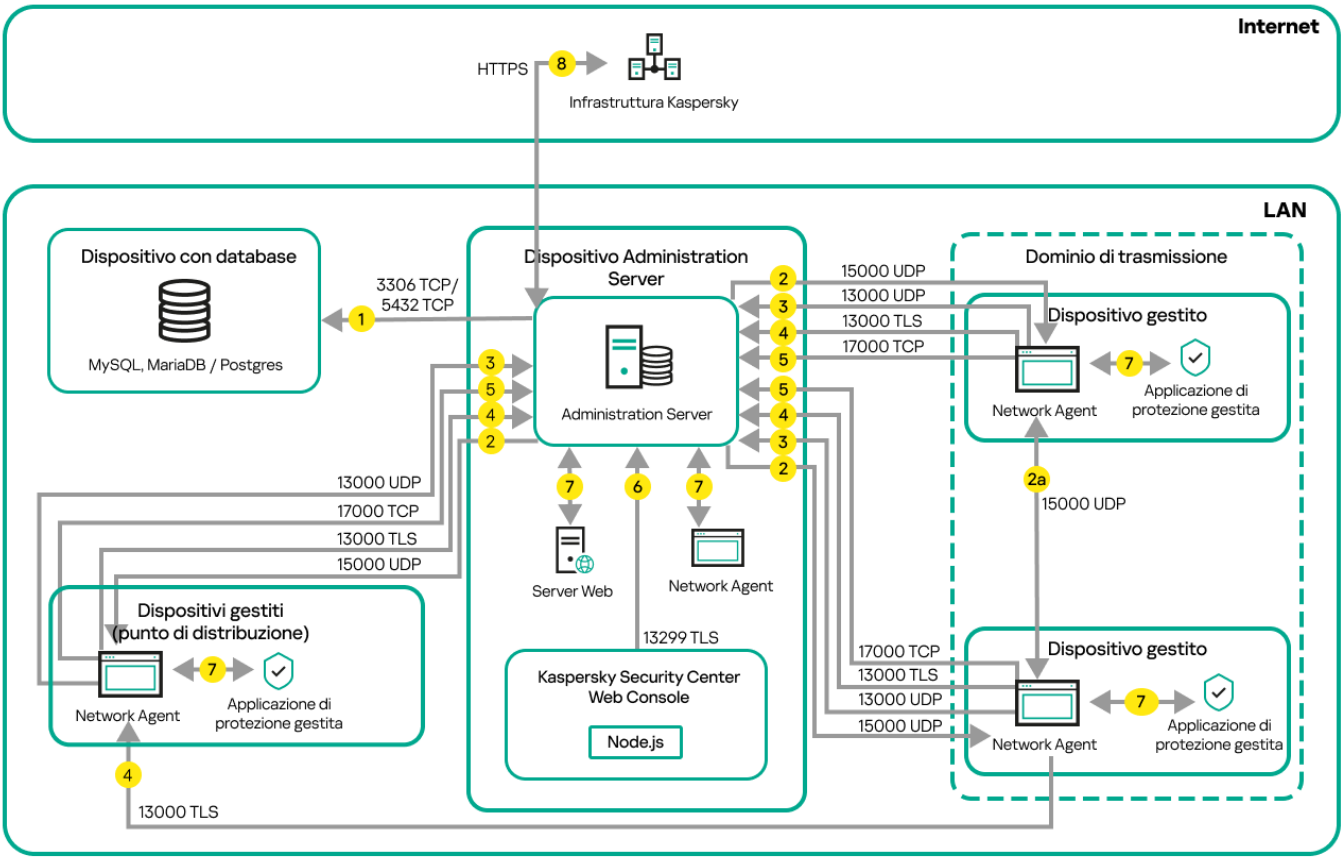
- È inoltre possibile utilizzare gateway di connessione all'interno della rete. I punti di distribuzione assegnati automaticamente diventano ad esempio anche gateway di connessione nel proprio ambito. Tuttavia, all'interno di una rete interna, i gateway di connessione non offrono vantaggi considerevoli. Riducono il numero di connessioni di rete ricevute da Administration Server, ma non riducono il volume dei dati in entrata. Anche senza gateway di connessione tutti i dispositivi potrebbero comunque connettersi ad Administration Server.

Schemi per traffico dati e utilizzo delle porte

Questa sezione fornisce schemi per il traffico dati tra i componenti di Kaspersky Security Center Linux, le applicazioni di protezione gestite e i server esterni in varie configurazioni. Gli schemi vengono forniti con i numeri delle porte che devono essere disponibili nei dispositivi locali.

Administration Server e dispositivi gestiti nella LAN

La figura di seguito mostra il traffico dati se Kaspersky Security Center è distribuito solo in una LAN (Local Area Network).



Administration Server e i dispositivi gestiti in una LAN (Local Area Network)

La figura illustra come diversi dispositivi gestiti si connettono all'Administration Server in modi differenti: direttamente o tramite un punto di distribuzione. I punti di distribuzione riducono il carico sull'Administration Server durante la distribuzione degli aggiornamenti e ottimizzano il traffico di rete. Tuttavia, i punti di distribuzione sono necessari solo se il numero di dispositivi gestiti è sufficientemente elevato. Se il numero di dispositivi gestiti è limitato, i dispositivi gestiti possono ricevere gli aggiornamenti direttamente dall'Administration Server.

Le frecce indicano l'origine del traffico: ogni freccia punta da un dispositivo che avvia la connessione al dispositivo che "risponde" alla chiamata. Vengono forniti il numero della porta e il nome del protocollo utilizzato per il trasferimento dei dati. Ogni freccia ha un'etichetta numerica e i dettagli sul traffico dati corrispondente sono i seguenti:

1. Administration Server invia i dati al database. Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL e MariaDB o la porta 432 per PostgreSQL Server o Postgres Pro Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2. Le richieste di comunicazione provenienti da Administration Server vengono trasferite a tutti i dispositivi gestiti non mobili tramite la porta UDP 15000.

   I Network Agent inviano richieste reciproche con un solo dominio di trasmissione. I dati vengono quindi inviati ad Administration Server e utilizzati per definire i limiti del dominio di trasmissione e per l'assegnazione automatica dei punti di distribuzione (se questa opzione è abilitata).

   Se Administration Server non ha accesso diretto ai dispositivi gestiti, le richieste di comunicazione da Administration Server a questi dispositivi non vengono inviate direttamente.

   2a. I Network Agent nei dispositivi gestiti non mobili scambiano dati su altri Network Agent all'interno dello stesso dominio di trasmissione (i dati vengono quindi inviati ad Administration Server).

3. Le informazioni sull'arresto dei dispositivi gestiti vengono trasferite dal Network Agent all'Administration Server tramite la porta UDP 13000.

4. Administration Server riceve la connessione dai Network Agent e dagli Administration Server secondari tramite la porta TLS 13000.

   Se è stata utilizzata una versione precedente di Kaspersky Security Center, l'Administration Server nella rete può ricevere la connessione dai Network Agent tramite la porta non TLS 14000. Kaspersky Security Center supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta TLS 13000.

5. I dispositivi gestiti (ad eccezione dei dispositivi mobili) richiedono l'attivazione tramite la porta TCP 17000. Ciò non è necessario se il dispositivo dispone già dell'accesso a Internet; in tal caso il dispositivo invia i dati ai server Kaspersky direttamente via Internet.

6. Kaspersky Security Center Web Console Server invia i dati all'Administration Server, che può essere installato nello stesso dispositivo o in un altro dispositivo, tramite la porta TLS 13299.

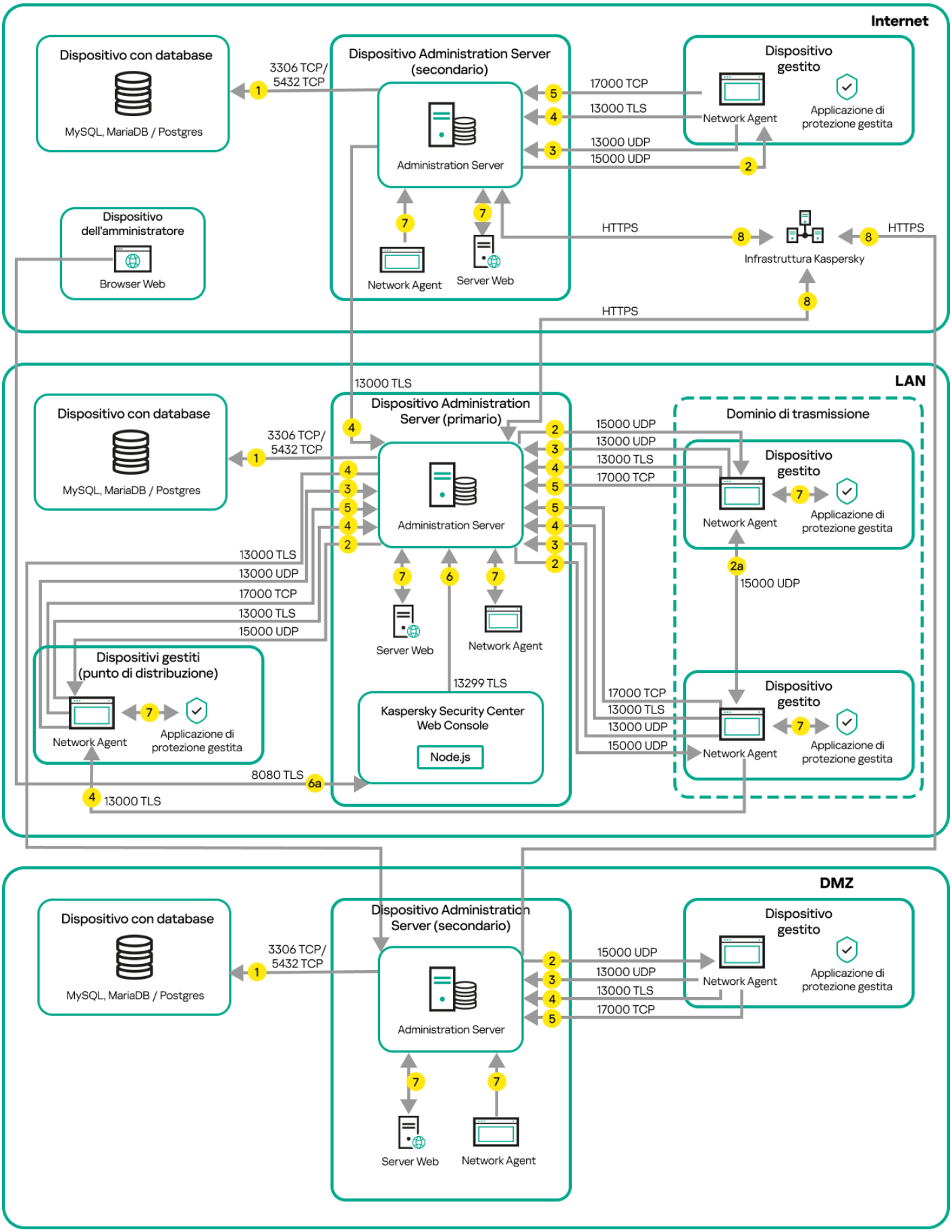
7. Nelle applicazioni presenti in un singolo dispositivo avviene lo scambio di traffico locale (nell'Administration Server o in un dispositivo gestito). Non è necessaria l'apertura di porte esterne.

8. Il dati inviati dall'Administration Server ai server Kaspersky (ad esempio, i dati KSN o le informazioni sulle licenze) e i dati inviati dai server Kaspersky all'Administration Server (ad esempio, gli aggiornamenti delle applicazioni e dei database anti-virus) vengono trasferiti tramite il protocollo HTTPS.

   Se non si desidera concedere all'Administration Server l'accesso a Internet, è necessario gestire questi dati manualmente.

Administration Server primario nella LAN e due Administration Server secondari

La figura di seguito mostra la gerarchia degli Administration Server: l'Administration Server primario si trova in una LAN. Un Administration Server secondario si trova in una rete perimetrale; un altro Administration Server secondario si trova in Internet.



Gerarchia degli Administration Server: Administration Server primario e due Administration Server secondari

Le frecce indicano l'origine del traffico: ogni freccia punta da un dispositivo che avvia la connessione al dispositivo che "risponde" alla chiamata. Vengono forniti il numero della porta e il nome del protocollo utilizzato per il trasferimento dei dati. Ogni freccia ha un'etichetta numerica e i dettagli sul traffico dati corrispondente sono i seguenti:

1. Administration Server invia i dati al database. Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL e MariaDB o la porta 432 per PostgreSQL Server o Postgres Pro Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2. Le richieste di comunicazione provenienti da Administration Server vengono trasferite a tutti i dispositivi gestiti non mobili tramite la porta UDP 15000.

   I Network Agent inviano richieste reciproche con un solo dominio di trasmissione. I dati vengono quindi inviati ad Administration Server e utilizzati per definire i limiti del dominio di trasmissione e per l'assegnazione automatica dei punti di distribuzione (se questa opzione è abilitata).

   Se Administration Server non ha accesso diretto ai dispositivi gestiti, le richieste di comunicazione da Administration Server a questi dispositivi non vengono inviate direttamente.

3. Le informazioni sull'arresto dei dispositivi gestiti vengono trasferite dal Network Agent all'Administration Server tramite la porta UDP 13000.

4. Administration Server riceve la connessione dai Network Agent e dagli Administration Server secondari tramite la porta TLS 13000.

   Se è stata utilizzata una versione precedente di Kaspersky Security Center, l'Administration Server nella rete può ricevere la connessione dai Network Agent tramite la porta non TLS 14000. Kaspersky Security Center Linux supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta TLS 13000.

5. I dispositivi gestiti (ad eccezione dei dispositivi mobili) richiedono l'attivazione tramite la porta TCP 17000. Ciò non è necessario se il dispositivo dispone già dell'accesso a Internet; in tal caso il dispositivo invia i dati ai server Kaspersky direttamente via Internet.

6. Kaspersky Security Center Web Console Server invia i dati all'Administration Server, che può essere installato nello stesso dispositivo o in un altro dispositivo, tramite la porta TLS 13299.

   6a. I dati provenienti dal browser, installato in un altro dispositivo dell'amministratore, vengono trasferiti a Kaspersky Security Center Web Console Server tramite la porta TLS 8080. Kaspersky Security Center Web Console Server può essere installato in Administration Server o in un altro dispositivo.

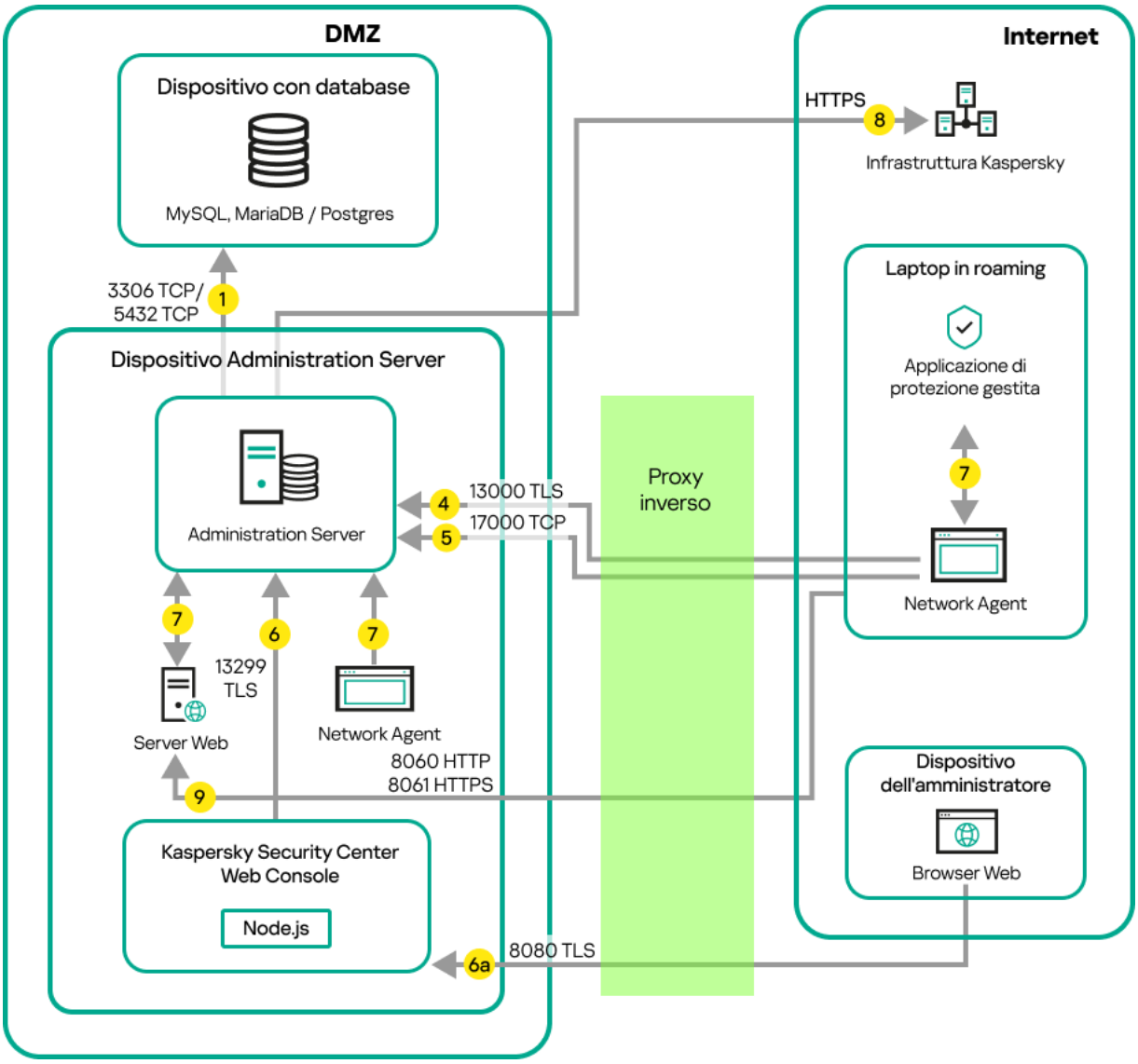
7. Nelle applicazioni presenti in un singolo dispositivo avviene lo scambio di traffico locale (nell'Administration Server o in un dispositivo gestito). Non è necessaria l'apertura di porte esterne.

8. Il dati inviati dall'Administration Server ai server Kaspersky (ad esempio, i dati KSN o le informazioni sulle licenze) e i dati inviati dai server Kaspersky all'Administration Server (ad esempio, gli aggiornamenti delle applicazioni e dei database anti-virus) vengono trasferiti tramite il protocollo HTTPS.

   Se non si desidera concedere all'Administration Server l'accesso a Internet, è necessario gestire questi dati manualmente.

Administration Server nella LAN, dispositivi gestiti in Internet, proxy inverso in uso

La figura di seguito mostra il traffico dati se Administration Server si trova all'interno di una LAN e i dispositivi gestiti sono in Internet. In questa figura, è in uso un proxy inverso a scelta. Per informazioni dettagliate, fare riferimento alla documentazione dell'applicazione.



Administration Server in una LAN; i dispositivi gestiti si connettono all'Administration Server tramite un proxy inverso

Questo schema di distribuzione è consigliabile se non si desidera che i dispositivi mobili si connettano direttamente all'Administration Server e non si desidera assegnare un gateway di connessione nella rete perimetrale.

Le frecce indicano l'origine del traffico: ogni freccia punta da un dispositivo che avvia la connessione al dispositivo che "risponde" alla chiamata. Vengono forniti il numero della porta e il nome del protocollo utilizzato per il trasferimento dei dati. Ogni freccia ha un'etichetta numerica e i dettagli sul traffico dati corrispondente sono i seguenti:

1. Administration Server invia i dati al database. Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL e MariaDB o la porta 432 per PostgreSQL Server o Postgres Pro Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2. Le richieste di comunicazione provenienti da Administration Server vengono trasferite a tutti i dispositivi gestiti non mobili tramite la porta UDP 15000.

   I Network Agent inviano richieste reciproche con un solo dominio di trasmissione. I dati vengono quindi inviati ad Administration Server e utilizzati per definire i limiti del dominio di trasmissione e per l'assegnazione automatica dei punti di distribuzione (se questa opzione è abilitata).

   Se Administration Server non ha accesso diretto ai dispositivi gestiti, le richieste di comunicazione da Administration Server a questi dispositivi non vengono inviate direttamente.

3. Le informazioni sull'arresto dei dispositivi gestiti vengono trasferite dal Network Agent all'Administration Server tramite la porta UDP 13000.

4. Administration Server riceve la connessione dai Network Agent e dagli Administration Server secondari tramite la porta TLS 13000.

   Se è stata utilizzata una versione precedente di Kaspersky Security Center, l'Administration Server nella rete può ricevere la connessione dai Network Agent tramite la porta non TLS 14000. Kaspersky Security Center Linux supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta TLS 13000.

5. I dispositivi gestiti (ad eccezione dei dispositivi mobili) richiedono l'attivazione tramite la porta TCP 17000. Ciò non è necessario se il dispositivo dispone già dell'accesso a Internet; in tal caso il dispositivo invia i dati ai server Kaspersky direttamente via Internet.

6. Kaspersky Security Center Web Console Server invia i dati all'Administration Server, che può essere installato nello stesso dispositivo o in un altro dispositivo, tramite la porta TLS 13299.

   6a. I dati provenienti dal browser, installato in un altro dispositivo dell'amministratore, vengono trasferiti a Kaspersky Security Center Web Console Server tramite la porta TLS 8080. Kaspersky Security Center Web Console Server può essere installato in Administration Server o in un altro dispositivo.

7. Nelle applicazioni presenti in un singolo dispositivo avviene lo scambio di traffico locale (nell'Administration Server o in un dispositivo gestito). Non è necessaria l'apertura di porte esterne.

8. Il dati inviati dall'Administration Server ai server Kaspersky (ad esempio, i dati KSN o le informazioni sulle licenze) e i dati inviati dai server Kaspersky all'Administration Server (ad esempio, gli aggiornamenti delle applicazioni e dei database anti-virus) vengono trasferiti tramite il protocollo HTTPS.

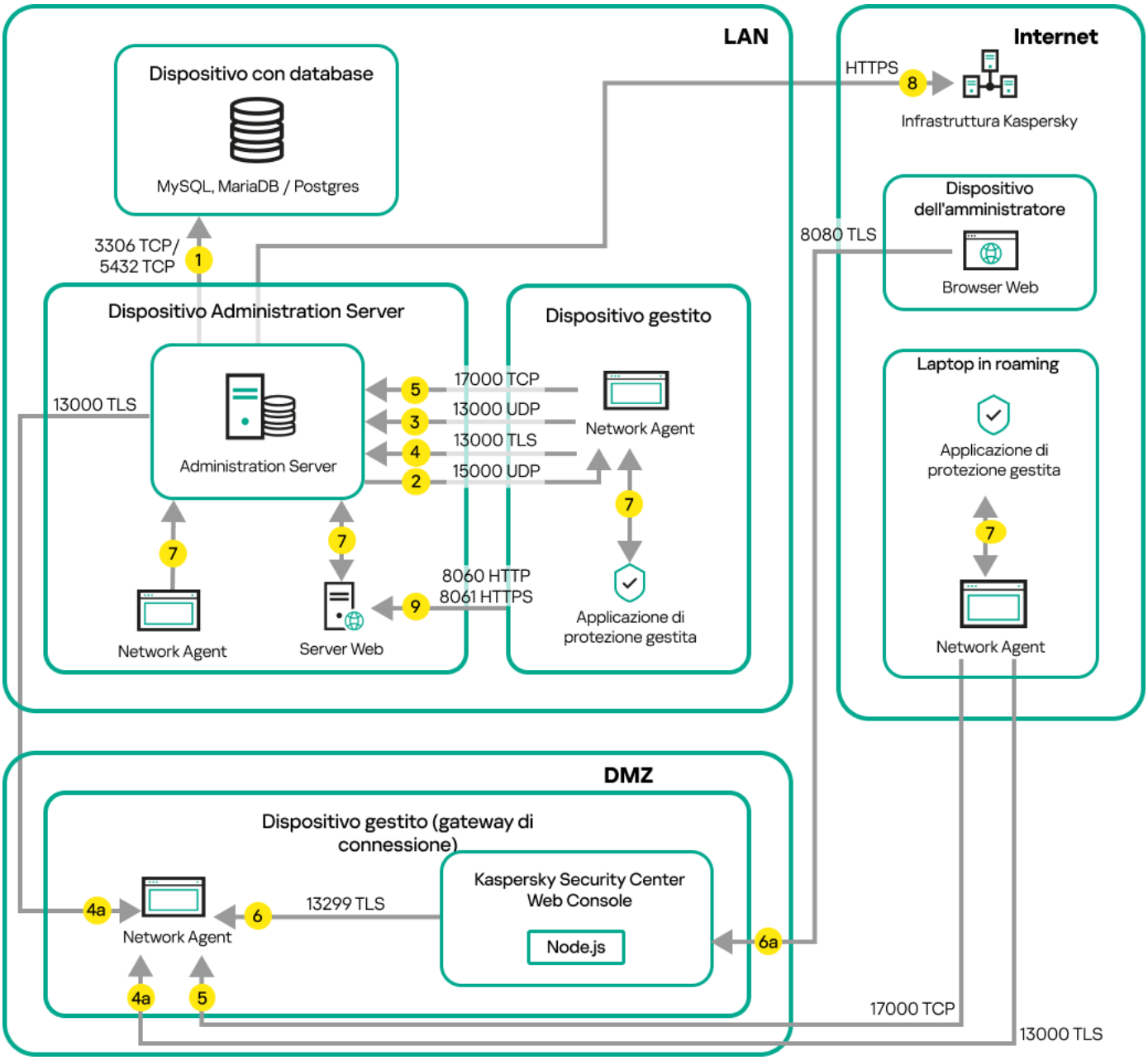
   Se non si desidera concedere all'Administration Server l'accesso a Internet, è necessario gestire questi dati manualmente.

9. Le richieste di pacchetti provenienti dai dispositivi gestiti, inclusi i dispositivi mobili, vengono trasferite al server Web, che si trova nello stesso dispositivo in cui si trova Administration Server.

Administration Server nella LAN, dispositivi gestiti in Internet, gateway di connessione in uso

La figura di seguito mostra il traffico dati se Administration Server si trova all'interno di una LAN e i dispositivi gestiti sono in Internet. È in uso un gateway di connessione.

Questo schema di distribuzione è consigliabile se non si desidera che i dispositivi gestiti si connettano direttamente all'Administration Server e non si desidera utilizzare un proxy inverso o un firewall aziendale.



Dispositivi mobili gestiti connessi all'Administration Server tramite un gateway di connessione

In questa figura i dispositivi gestiti sono connessi all'Administration Server tramite un gateway di connessione che si trova nella rete perimetrale. Non è in uso alcun proxy inverso o firewall aziendale.

Le frecce indicano l'origine del traffico: ogni freccia punta da un dispositivo che avvia la connessione al dispositivo che "risponde" alla chiamata. Vengono forniti il numero della porta e il nome del protocollo utilizzato per il trasferimento dei dati. Ogni freccia ha un'etichetta numerica e i dettagli sul traffico dati corrispondente sono i seguenti:

1. Administration Server invia i dati al database. Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL e MariaDB o la porta 432 per PostgreSQL Server o Postgres Pro Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2. Le richieste di comunicazione provenienti da Administration Server vengono trasferite a tutti i dispositivi gestiti non mobili tramite la porta UDP 15000.

   I Network Agent inviano richieste reciproche con un solo dominio di trasmissione. I dati vengono quindi inviati ad Administration Server e utilizzati per definire i limiti del dominio di trasmissione e per l'assegnazione automatica dei punti di distribuzione (se questa opzione è abilitata).

Se Administration Server non ha accesso diretto ai dispositivi gestiti, le richieste di comunicazione da Administration Server a questi dispositivi non vengono inviate direttamente.

3. Le informazioni sull'arresto dei dispositivi gestiti vengono trasferite dal Network Agent all'Administration Server tramite la porta UDP 13000.

4. Administration Server riceve la connessione dai Network Agent e dagli Administration Server secondari tramite la porta TLS 13000.

   Se è stata utilizzata una versione precedente di Kaspersky Security Center, l'Administration Server nella rete può ricevere la connessione dai Network Agent tramite la porta non TLS 14000. Kaspersky Security Center Linux supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta TLS 13000.

   4a. Anche un gateway di connessione nella rete perimetrale riceve la connessione da Administration Server tramite la porta TLS 13000. Dal momento che un gateway di connessione nella rete perimetrale non può raggiungere le porte di Administration Server, Administration Server crea e mantiene una connessione di segnale permanente con un gateway di connessione. La connessione di segnale non viene utilizzata per il trasferimento dei dati; viene utilizzata solo per inviare un invito all'interazione di rete. Quando deve connettersi al server, il gateway di connessione invia una notifica al server attraverso questa connessione di segnale, quindi il server crea la connessione richiesta per il trasferimento dei dati.

   Anche i dispositivi fuori sede si connettono al gateway di connessione tramite la porta TLS 13000.

5. I dispositivi gestiti (ad eccezione dei dispositivi mobili) richiedono l'attivazione tramite la porta TCP 17000. Ciò non è necessario se il dispositivo dispone già dell'accesso a Internet; in tal caso il dispositivo invia i dati ai server Kaspersky direttamente via Internet.

6. Kaspersky Security Center Web Console Server invia i dati all'Administration Server, che può essere installato nello stesso dispositivo o in un altro dispositivo, tramite la porta TLS 13299.

   6a. I dati provenienti dal browser, installato in un altro dispositivo dell'amministratore, vengono trasferiti a Kaspersky Security Center Web Console Server tramite la porta TLS 8080. Kaspersky Security Center Web Console Server può essere installato in Administration Server o in un altro dispositivo.

7. Nelle applicazioni presenti in un singolo dispositivo avviene lo scambio di traffico locale (nell'Administration Server o in un dispositivo gestito). Non è necessaria l'apertura di porte esterne.

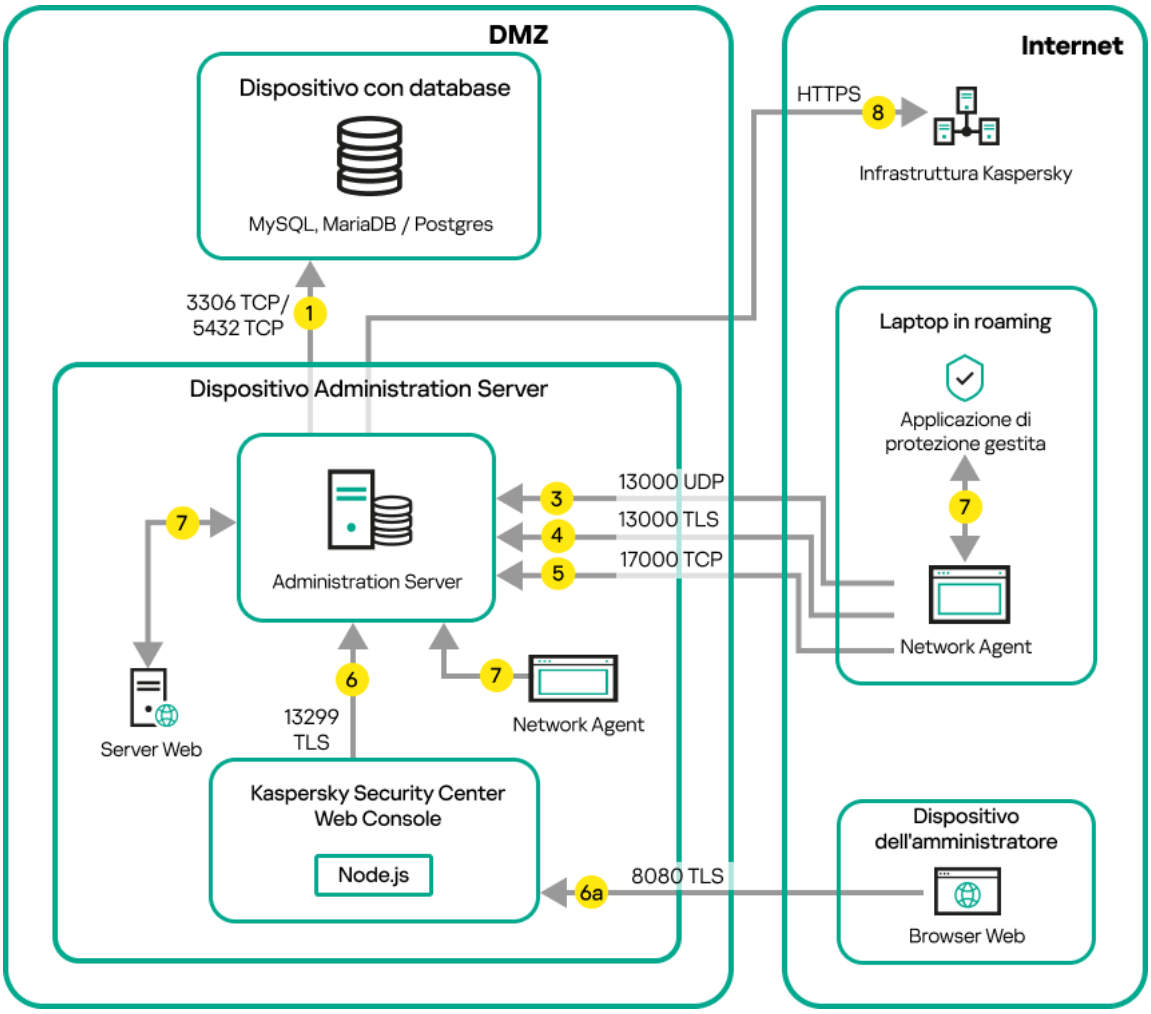
8. Il dati inviati dall'Administration Server ai server Kaspersky (ad esempio, i dati KSN o le informazioni sulle licenze) e i dati inviati dai server Kaspersky all'Administration Server (ad esempio, gli aggiornamenti delle applicazioni e dei database anti-virus) vengono trasferiti tramite il protocollo HTTPS.

   Se non si desidera concedere all'Administration Server l'accesso a Internet, è necessario gestire questi dati manualmente.

9. Le richieste di pacchetti provenienti dai dispositivi gestiti, inclusi i dispositivi mobili, vengono trasferite al server Web, che si trova nello stesso dispositivo in cui si trova Administration Server.

Administration Server all'interno della rete perimetrale, dispositivi gestiti in Internet

La figura di seguito mostra il traffico dati se l'Administration Server si trova nella rete perimetrale (DMZ) e i dispositivi gestiti sono in Internet.



Administration Server nella rete perimetrale, dispositivi mobili gestiti in Internet

In questa figura non è in uso alcun gateway di connessione: i dispositivi mobili si connettono direttamente all'Administration Server.

Le frecce indicano l'origine del traffico: ogni freccia punta da un dispositivo che avvia la connessione al dispositivo che "risponde" alla chiamata. Vengono forniti il numero della porta e il nome del protocollo utilizzato per il trasferimento dei dati. Ogni freccia ha un'etichetta numerica e i dettagli sul traffico dati corrispondente sono i seguenti:

1. Administration Server invia i dati al database. Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL e MariaDB o la porta 432 per PostgreSQL Server o Postgres Pro Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2. Le richieste di comunicazione provenienti da Administration Server vengono trasferite a tutti i dispositivi gestiti non mobili tramite la porta UDP 15000.

   I Network Agent inviano richieste reciproche con un solo dominio di trasmissione. I dati vengono quindi inviati ad Administration Server e utilizzati per definire i limiti del dominio di trasmissione e per l'assegnazione automatica dei punti di distribuzione (se questa opzione è abilitata).

   Se Administration Server non ha accesso diretto ai dispositivi gestiti, le richieste di comunicazione da Administration Server a questi dispositivi non vengono inviate direttamente.

3. Le informazioni sull'arresto dei dispositivi gestiti vengono trasferite dal Network Agent all'Administration Server tramite la porta UDP 13000.

4. Administration Server riceve la connessione dai Network Agent e dagli Administration Server secondari tramite la porta TLS 13000.

Se è stata utilizzata una versione precedente di Kaspersky Security Center, l'Administration Server nella rete può ricevere la connessione dai Network Agent tramite la porta non TLS 14000. Kaspersky Security Center Linux supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta TLS 13000.

5. I dispositivi gestiti (ad eccezione dei dispositivi mobili) richiedono l'attivazione tramite la porta TCP 17000. Ciò non è necessario se il dispositivo dispone già dell'accesso a Internet; in tal caso il dispositivo invia i dati ai server Kaspersky direttamente via Internet.

6. Kaspersky Security Center Web Console Server invia i dati all'Administration Server, che può essere installato nello stesso dispositivo o in un altro dispositivo, tramite la porta TLS 13299.

   6a. I dati provenienti dal browser, installato in un altro dispositivo dell'amministratore, vengono trasferiti a Kaspersky Security Center Web Console Server tramite la porta TLS 8080. Kaspersky Security Center Web Console Server può essere installato in Administration Server o in un altro dispositivo.

7. Nelle applicazioni presenti in un singolo dispositivo avviene lo scambio di traffico locale (nell'Administration Server o in un dispositivo gestito). Non è necessaria l'apertura di porte esterne.

8. Il dati inviati dall'Administration Server ai server Kaspersky (ad esempio, i dati KSN o le informazioni sulle licenze) e i dati inviati dai server Kaspersky all'Administration Server (ad esempio, gli aggiornamenti delle applicazioni e dei database anti-virus) vengono trasferiti tramite il protocollo HTTPS.

   Se non si desidera concedere all'Administration Server l'accesso a Internet, è necessario gestire questi dati manualmente.

9. Le richieste di pacchetti provenienti dai dispositivi gestiti vengono trasferite al server Web, che si trova nello stesso dispositivo in cui si trova Administration Server.

Interazione dei componenti di Kaspersky Security Center Linux e delle applicazioni di protezione: ulteriori informazioni

In questa sezione vengono forniti gli schemi per l'interazione dei componenti di Kaspersky Security Center Linux e delle applicazioni di protezione gestite. Gli schemi forniscono i numeri delle porte che devono essere disponibili e i nomi dei processi che aprono tali porte.

Convenzioni utilizzate negli schemi di interazione

Nella seguente tabella sono fornite le convenzioni utilizzate negli schemi.

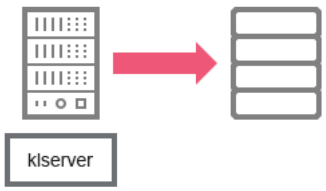
Convenzioni utilizzate nella documentazione

Icona	Significato
	Administration Server
	Administration Server secondario
	DBMS

	Dispositivo client (in cui sono installati Network Agent e un'applicazione della famiglia Kaspersky Endpoint Security o un'altra applicazione di protezione che può essere gestita da Kaspersky Security Center Linux)
	Gateway di connessione
	Punto di distribuzione
	Browser nel dispositivo dell'utente
	Processo in esecuzione nel dispositivo e apertura di una porta
	Porta e relativo numero
	Traffico TCP (la direzione della freccia indica la direzione del flusso di traffico)
	Traffico UDP (la direzione della freccia indica la direzione del flusso di traffico)
	Trasporto DBMS
	Limite della rete perimetrale

Administration Server e DBMS

I dati provenienti da Administration Server vengono immessi in un database.

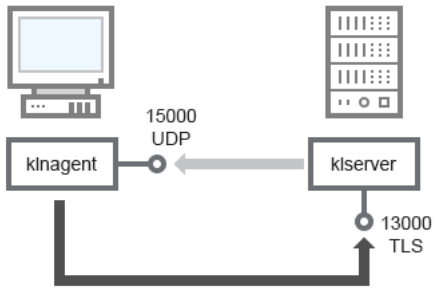


Administration Server e DBMS

Se si installano l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per MariaDB). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

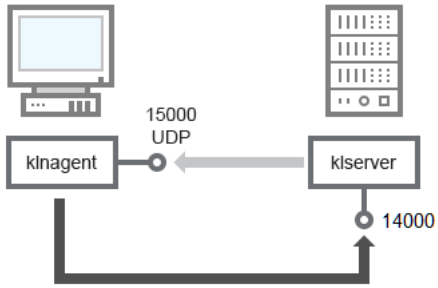
Administration Server e dispositivo client: gestione dell'applicazione di protezione

L'Administration Server riceve la connessione dai Network Agent tramite la porta TLS 13000 (vedere la figura seguente).



Administration Server e dispositivo client: gestione dell'applicazione di protezione, connessione tramite la porta 13000 (consigliata)

Se è stata utilizzata una versione precedente di Kaspersky Security Center Linux, Administration Server nella rete può ricevere connessioni dai Network Agent tramite la porta non SSL 14000 (vedere la figura seguente). Kaspersky Security Center Linux supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta SSL 13000.



Administration Server e dispositivo client: gestione dell'applicazione di protezione, connessione tramite la porta 14000 (protezione inferiore)

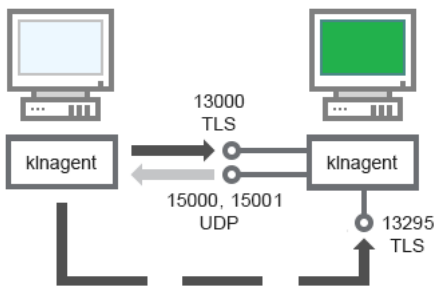
Per le spiegazioni degli schemi, vedere la tabella seguente.

Administration Server e dispositivo client: gestione dell'applicazione di protezione (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta
Network Agent	15000	klnagent	UDP	Multicasting per Network Agent
Administration Server	13000	klserver	TCP (TLS)	Ricezione delle connessioni dai Network Agent
Administration Server	14000	klserver	TCP	Ricezione delle connessioni dai Network Agent

Upgrade del software in un dispositivo client tramite un punto di distribuzione

Il dispositivo client si connette al punto di distribuzione tramite la porta 13000 e, se si utilizza il punto di distribuzione come server push, anche tramite la porta 13295; il punto di distribuzione esegue la distribuzione multicast ai Network Agent tramite la porta 15000 (vedere la figura seguente). Gli aggiornamenti e i pacchetti di installazione vengono ricevuti da un punto di distribuzione tramite la porta 15001.



Per dettagli sullo schema, vedere la tabella di seguito.

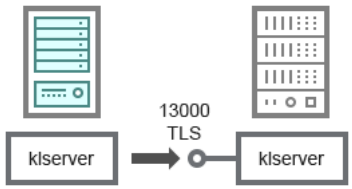
Upgrade del software tramite un punto di distribuzione (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta
Network Agent	15000	klnagent	UDP	Multicasting per Network Agent
Network Agent	15001	klnagent	UDP	Ricezione di aggiornamenti e pacchetti di installazione da un punto di distribuzione
Punto di distribuzione	13000	klnagent	TCP (TLS)	Ricezione delle connessioni dai Network Agent
Punto di distribuzione	13295	klnagent	TCP (TLS)	Ricezione di connessioni dai dispositivi client (server push)

Gerarchia di Administration Server: Administration Server primario e Administration Server secondario

Lo schema (vedere la figura seguente) illustra come utilizzare la porta 13000 per garantire l'interazione tra più Administration Server combinati in una gerarchia.

Successivamente, una volta che gli Administration Server sono combinati in una gerarchia, sarà possibile amministrarli entrambi utilizzando Kaspersky Security Center Web Console connesso all'Administration Server primario. Di conseguenza, l'unico prerequisito è l'accessibilità della porta 13299 dell'Administration Server primario.



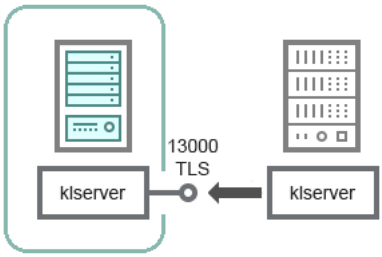
Gerarchia di Administration Server: Administration Server primario e Administration Server secondario

Per dettagli sullo schema, vedere la tabella di seguito.

Gerarchia di Administration Server (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta
Administration Server primario	13000	klserver	TCP (TLS)	Ricezione delle connessioni dagli Administration Server secondari

Gerarchia di Administration server con un Administration Server secondario nella rete perimetrale



Gerarchia di Administration server con un Administration Server secondario nella rete perimetrale

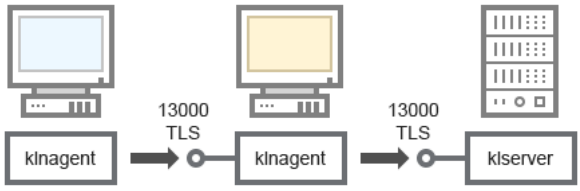
Lo schema illustra una gerarchia di Administration Server in cui l'Administration Server secondario disponibile nella rete perimetrale riceve una connessione dall'Administration Server primario (vedere la tabella seguente per le spiegazioni dello schema). Quando si combinano due Administration Server in una gerarchia, verificare che la porta 13299 sia accessibile in entrambi gli Administration Server. Kaspersky Security Center Web Console si connette ad Administration Server tramite la porta 13299.

Successivamente, una volta che gli Administration Server sono combinati in una gerarchia, sarà possibile amministrarli entrambi utilizzando Kaspersky Security Center Web Console connesso all'Administration Server primario. Di conseguenza, l'unico prerequisito è l'accessibilità della porta 13299 dell'Administration Server primario.

Gerarchia di Administration Server con un Administration Server secondario nella rete perimetrale (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta
Administration Server secondario	13000	klserver	TCP (TLS)	Ricezione delle connessioni dall'Administration Server primario

Administration Server, un gateway di connessione in un segmento di rete e un dispositivo client



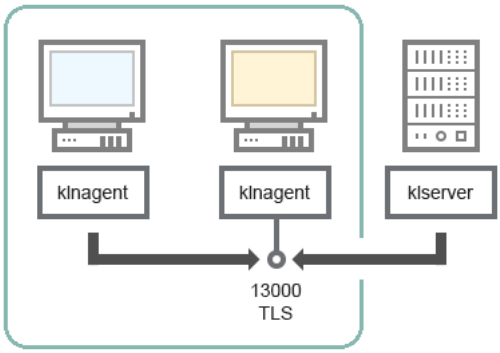
Administration Server, un gateway di connessione in un segmento di rete e un dispositivo client

Per dettagli sullo schema, vedere la tabella di seguito.

Administration Server, un gateway di connessione in un segmento di rete e un dispositivo client (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta
Administration Server	13000	klserver	TCP (TLS)	Ricezione delle connessioni dai Network Agent
Network Agent	13000	klnagent	TCP (TLS)	Ricezione delle connessioni dai Network Agent

Administration Server e due dispositivi nella rete perimetrale: un gateway di connessione e un dispositivo client



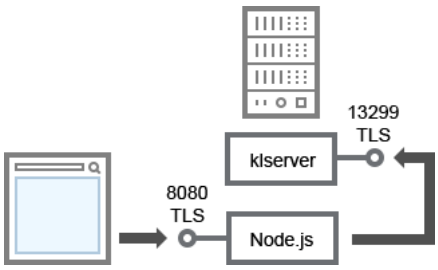
Administration Server con un gateway di connessione e un dispositivo client nella rete perimetrale

Per dettagli sullo schema, vedere la tabella di seguito.

Administration Server con un gateway di connessione in un segmento di rete e un dispositivo client (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta
Network Agent	13000	klnagent	TCP (TLS)	Ricezione delle connessioni dai Network Agent

Administration Server e Kaspersky Security Center Web Console



Administration Server e Kaspersky Security Center Web Console

Per dettagli sullo schema, vedere la tabella di seguito.

Administration Server e Kaspersky Security Center Web Console (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta
Administration Server	13299	klserver	TCP (TLS)	Ricezione delle connessioni da Kaspersky Security Center Web Console ad Administration Server tramite OpenAPI
Kaspersky Security Center Web Console Server o Administration Server	8080	Node.js: Server-side JavaScript	TCP (TLS)	Ricezione delle connessioni da Kaspersky Security Center Web Console

Kaspersky Security Center Web Console può essere installato in Administration Server o in un altro dispositivo.

Operazioni preliminari

Tramite questo scenario è possibile installare Kaspersky Security Center Linux Administration Server e Kaspersky Security Center Web Console, eseguire la configurazione iniziale di Administration Server tramite l'avvio rapido guidato e installare le applicazioni Kaspersky nei dispositivi gestiti utilizzando la Distribuzione guidata della protezione.

Prerequisiti

È necessario disporre di una chiave di licenza (codice di attivazione) per Kaspersky Endpoint Security for Business o di chiavi di licenza (codici di attivazione) per le applicazioni di protezione Kaspersky.

Se si desidera provare prima Kaspersky Security Center Linux, è possibile ottenere una prova gratuita di 30 giorni nel sito Web di Kaspersky.

Passaggi

Lo scenario di installazione principale procede per fasi:

1. **Selezione di una struttura per la protezione di un'organizzazione**

   Ulteriori informazioni sui componenti di Kaspersky Security Center Linux. In base alla configurazione di rete e al throughput dei canali di comunicazione, definire il numero di Administration Server da utilizzare e come devono essere distribuiti tra le varie sedi (se si esegue una rete distribuita).

   Definire se utilizzare o meno una gerarchia di Administration Server nell'organizzazione. A tale scopo, è necessario valutare se è possibile e conveniente coprire tutti i dispositivi client con un singolo Administration Server o se è necessario creare una gerarchia di Administration Server. Può inoltre essere necessario creare una gerarchia di Administration Server che corrisponda perfettamente alla struttura organizzativa dell'organizzazione per cui si desidera proteggere la rete.

2. **Preparazione per l'utilizzo dei certificati personalizzati**

   Se l'infrastruttura a chiave pubblica (PKI) dell'organizzazione richiede l'utilizzo di certificati personalizzati emessi da un'autorità di certificazione specifica, preparare tali certificati e assicurarsi che soddisfino tutti i requisiti.

3. **Installazione di un sistema di gestione database (DBMS)**

   Installare il DBMS che verrà utilizzato da Kaspersky Security Center Linux o utilizzarne uno esistente.

   È possibile scegliere uno dei DBMS supportati. Per informazioni su come installare il DBMS selezionato, consultare la relativa documentazione.

   Se la distribuzione del sistema operativo basato su Linux non contiene un DBMS supportato, è possibile installare il DBMS da un archivio di pacchetti di terzi. Se l'installazione di distribuzioni da archivi di terzi è vietata, è possibile installare il DBMS in un dispositivo separato.

   > Se si decide di installare il DBMS di PostgreSQL o Postgres Pro, assicurarsi di aver specificato una password per il l'utente con privilegi avanzati. Se la password non viene specificata, Administration Server potrebbe non essere in grado di connettersi al database.

   Se si installa MariaDB, PostgreSQL o Postgres Pro, utilizzare le impostazioni consigliate per garantire il corretto funzionamento del DBMS.

Se si desidera modificare il tipo di DBMS dopo l'installazione, è necessario reinstallare Kaspersky Security Center Linux. I dati possono essere parzialmente e manualmente trasferiti a un altro database.

4. **Configurazione delle porte**

   Verificare che tutte le porte necessarie siano aperte per l'interazione tra i componenti in base della struttura di protezione selezionata.

   Se è necessario concedere ad Administration Server l'accesso a Internet, configurare le porte e specificare le impostazioni di connessione, a seconda della configurazione di rete.

5. **Installazione di Kaspersky Security Center Linux**

   Selezionare un dispositivo Linux che si intende utilizzare come Administration Server, assicurarsi che il dispositivo soddisfi i requisiti software e hardware, quindi installare Kaspersky Security Center Linux nel dispositivo. La versione server di Network Agent è installata automaticamente insieme ad Administration Server.

6. **Installazione di Kaspersky Security Center Web Console e dei plug-in Web di gestione**

   Selezionare un dispositivo Linux che si intende utilizzare come workstation dell'amministratore, assicurarsi che il dispositivo soddisfi i requisiti software e hardware, quindi installare Kaspersky Security Center Web Console nel dispositivo. È possibile installare Kaspersky Security Center Web Console nello stesso dispositivo in cui è installato Administration Server o in un altro dispositivo.

   Scaricare il plug-in Web di gestione di Kaspersky Endpoint Security for Linux e installarlo nello stesso dispositivo in cui è installato Kaspersky Security Center Web Console.

7. **Installazione di Kaspersky Endpoint Security for Linux e Network Agent nel dispositivo Administration Server**

   Per impostazione predefinita, l'applicazione non considera il dispositivo Administration Server come dispositivo gestito. Per proteggere Administration Server da virus e altre minacce, nonché per gestire il dispositivo come qualsiasi altro dispositivo gestito, è consigliabile installare Kaspersky Endpoint Security for Linux e Network Agent per Linux nel dispositivo Administration Server. In questo caso, Network Agent per Linux è installato e funziona indipendentemente dalla versione server di Network Agent installata insieme ad Administration Server.

8. **Esecuzione della configurazione iniziale**

   Quando l'installazione di Administration Server è completa, alla prima connessione ad Administration Server viene avviato automaticamente l'Avvio rapido guidato. Eseguire la configurazione iniziale di Administration Server in base ai requisiti esistenti. Durante la fase di configurazione iniziale, la procedura guidata utilizza le impostazioni predefinite per creare i criteri e le attività necessari per la distribuzione della protezione. Le impostazioni predefinite potrebbero tuttavia non essere ottimali per le esigenze dell'organizzazione. Se necessario, è possibile modificare le impostazioni dei criteri e delle attività.

9. **Individuazione dei dispositivi nella rete**

   Individuare i dispositivi manualmente. Kaspersky Security Center Linux riceve gli indirizzi e i nomi di tutti i dispositivi rilevati nella rete. È quindi possibile utilizzare Kaspersky Security Center Linux per installare le applicazioni Kaspersky e software di altri produttori nei dispositivi rilevati. Kaspersky Security Center Linux avvia periodicamente la device discovery, pertanto eventuali nuove istanze che compaiono nella rete verranno rilevate automaticamente.

10. **Organizzazione dei dispositivi in gruppi di amministrazione**

    In alcuni casi, la distribuzione della protezione nei dispositivi della rete nel modo più immediato può richiedere la suddivisione dell'intero pool di dispositivi in gruppi di amministrazione, tenendo conto della struttura dell'organizzazione. È possibile creare regole di spostamento al fine di distribuire i dispositivi tra i gruppi oppure distribuire manualmente i dispositivi. È possibile assegnare attività di gruppo per i gruppi di amministrazione, definire l'ambito dei criteri e assegnare i punti di distribuzione.

    Verificare che tutti i dispositivi gestiti siano stati assegnati correttamente ai gruppi di amministrazione appropriati e che non siano più presenti dispositivi non assegnati nella rete.

11 Assegnazione dei punti di distribuzione

I punti di distribuzione vengono assegnati automaticamente ai gruppi di amministrazione ma è possibile assegnarli manualmente, se necessario. È consigliabile utilizzare i punti di distribuzione nelle reti su vasta scala per ridurre il carico su Administration Server e nelle reti con una struttura distribuita per consentire ad Administration Server di accedere ai dispositivi (o ai gruppi di dispositivi) tramite canali a basso throughput.

12 Installazione di Network Agent e di applicazioni di protezione nei dispositivi in rete

La distribuzione della protezione in una rete aziendale implica l'installazione di Network Agent e delle applicazioni di protezione nei dispositivi rilevati da Administration Server durante la device discovery.

Per installare le applicazioni in remoto, eseguire la Distribuzione guidata della protezione.

Le applicazioni di protezione proteggono i dispositivi da virus e da altri programmi che costituiscono una minaccia. Network Agent garantisce la comunicazione tra il dispositivo e Administration Server. Le impostazioni di Network Agent vengono configurate automaticamente per impostazione predefinita.

Prima di iniziare a installare Network Agent e le applicazioni di protezione nei dispositivi nella rete, verificare che questi dispositivi siano accessibili (attivati).

13 Distribuzione delle chiavi di licenza ai dispositivi client

Distribuire le chiavi di licenza ai dispositivi client per attivare applicazioni di protezione gestite in tali dispositivi.

14 Configurazione dei criteri delle applicazioni Kaspersky

Per applicare differenti impostazioni dell'applicazione ai diversi dispositivi, è possibile utilizzare la gestione della protezione incentrata sui dispositivi e/o la gestione della protezione incentrata sugli utenti. La gestione della protezione incentrata sui dispositivi può essere implementata utilizzando criteri e attività. È possibile applicare le attività solo ai dispositivi che soddisfano condizioni specifiche. Per impostare le condizioni per il filtro dei dispositivi, utilizzare le selezioni dispositivi e i tag.

15 Monitoraggio dello stato della protezione della rete

È possibile monitorare la rete utilizzando i widget nel dashboard, generare rapporti dalle applicazioni Kaspersky, configurare e visualizzare selezioni degli eventi ricevuti dalle applicazioni nei dispositivi gestiti e visualizzare elenchi di notifiche.

Installazione

Questa sezione descrive l'installazione di Kaspersky Security Center Linux e Kaspersky Security Center Web Console.

Configurazione del server MariaDB x64 per l'utilizzo con Kaspersky Security Center Linux

Impostazioni consigliate per il file my.cnf

Per maggiori dettagli sulla configurazione del DBMS, fare riferimento anche alla procedura di configurazione dell'account. Per informazioni sull'installazione del DBMS, fare riferimento alla procedura di installazione del DBMS.

Per configurare il file my.cnf:

1. Aprire il file my.cnf in un editor di testo.

2. Immettere le seguenti righe nella sezione [mysqld] del file my.cnf:

```
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=<valore>
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
```

Il valore di "`innodb_buffer_pool_size` non deve essere inferiore all'80% della dimensione del database KAV prevista. Si noti che la memoria specificata viene allocata all'avvio del server. Se la dimensione del database è inferiore alla dimensione del buffer specificata, viene allocata solo la memoria richiesta. Se si utilizza MariaDB 10.4.3 o versione precedente, la dimensione effettiva della memoria allocata è di circa il 10% maggiore rispetto alla dimensione del buffer specificata.

È consigliabile utilizzare il valore del parametro `innodb_flush_log_at_trx_commit=0`, perché i valori "1" o "2" influiscono negativamente sulla velocità di esecuzione di MariaDB. Assicurarsi che il parametro `innodb_file_per_table` sia impostato su `1`.

Per MariaDB 10.6, immettere inoltre le seguenti righe nella sezione [mysqld]:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Per impostazione predefinita, i componenti aggiuntivi dell'ottimizzatore `join_cache_incremental`, `join_cache_hashed` e `join_cache_bka` sono abilitati. Se questi componenti aggiuntivi non sono abilitati, è necessario abilitarli.

Per verificare se i componenti aggiuntivi dell'ottimizzatore sono abilitati:

1. Nella console del client MariaDB eseguire il comando:

```
SELECT @@optimizer_switch;
```

2. Verificare che l'output del comando contenga le seguenti righe:

```
join_cache_incremental=on
join_cache_hashed=on
join_cache_bka=on
```

Se queste righe sono presenti e hanno i valori `on`, i componenti aggiuntivi dell'ottimizzatore sono abilitati.

Se queste righe non sono presenti o hanno i valori `off`, è necessario eseguire le seguenti operazioni:

a. Aprire il file my.cnf in un editor di testo.

b. Aggiungere le seguenti righe nel file my.cnf:

```
optimizer_switch='join_cache_incremental=on'
optimizer_switch='join_cache_hashed=on'
optimizer_switch='join_cache_bka=on'
```

I componenti aggiuntivi `join_cache_incremental`, `join_cache_hash` e `join_cache_bka` vengono abilitati.

Configurazione del server PostgreSQL o Postgres per l'utilizzo con Kaspersky Security Center Linux

Kaspersky Security Center Linux supporta i DBMS PostgreSQL e Postgres Pro. Se si utilizza uno di questi DBMS, prendere in considerazione la configurazione dei parametri del server DBMS per ottimizzare il funzionamento del DBMS con Kaspersky Security Center Linux.

Il percorso predefinito del file di configurazione è: `/etc/postgresql/< VERSION >/main/postgresql.conf`

Parametri consigliati per PostgreSQL e Postgres Pro:

- `shared_buffers` = 25% del valore della RAM del dispositivo in cui è installato il DBMS

  Se la RAM è inferiore a 1 GB, lasciare il valore predefinito.

- `max_stack_depth` = dimensione massima dello stack (eseguire il comando '`ulimit -s`' per ottenere questo valore in KB) meno il margine di sicurezza di 1 MB

- `temp_buffers = 24MB`

- `work_mem = 16MB`

- `max_connections = 151`

- `max_parallel_workers_per_gather = 0`

- `maintenance_work_mem = 128MB`

Assicurarsi che il parametro `standard_conforming_strings` sia impostato sul valore predefinito `on`. Ricaricare la configurazione o riavviare il server dopo aver aggiornato il file postgresql.conf. Per ulteriori dettagli, consultare la documentazione di PostgreSQL.

Se si utilizza un cluster Postgres DBMS, specificare il parametro `max_connections` per tutti i server DBMS e nella configurazione del cluster.

Se si utilizza Postgres Pro 15.7 o Postgres Pro 15.7.1, disabilitare il parametro `enable_compound_index_stats`:

```
enable_compound_index_stats = off
```

Per informazioni dettagliate sui parametri dei server PostgreSQL e Postgres Pro e su come specificarli, fare riferimento alla documentazione del DBMS corrispondente.

Per ulteriori dettagli sulla creazione e la configurazione degli account per PostgreSQL e Postgres Pro, consultare il seguente argomento: Configurazione degli account per l'utilizzo di PostgreSQL e Postgres Pro.

Installazione di Kaspersky Security Center Linux

Questa procedura descrive come installare Kaspersky Security Center Linux.

Prima dell'installazione, è necessario:

- Installare un DBMS.
- Verificare che il dispositivo in cui si desidera installare Kaspersky Security Center Linux esegua una delle distribuzioni Linux supportate.
- Assicurarsi che il server DNS sia disponibile nella rete.

Usare il file di installazione—ksc64_[numero_versione]_amd64.deb or ksc64-[numero_versione].x86_64.rpm—che corrisponde alla distribuzione Linux installata nel dispositivo. È possibile ottenere il file di installazione scaricandolo dal sito Web di Kaspersky.

Per installare Kaspersky Security Center Linux, eseguire i comandi forniti nelle istruzioni seguenti con un account con privilegi di root.

Per installare Kaspersky Security Center Linux:

1. Se il dispositivo funziona con Astra Linux 1.8 o versione successiva, eseguire le azioni descritte in questo passaggio. Se il dispositivo viene eseguito su un sistema operativo diverso, procedere al passaggio successivo.

   a. Creare la directory /etc/systemd/system/kladminserver_srv.service.d e creare un file denominato override.conf con il seguente contenuto:
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Creare una directory /etc/systemd/system/klwebsrv_srv.service.d e creare un file denominato override.conf con il seguente contenuto:
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

2. Creare un gruppo "kladmins" e un account "ksc" senza privilegi. L'account deve essere un membro del gruppo "kladmins". A tale scopo, eseguire in sequenza i seguenti comandi:
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

3. Aumentare il limite predefinito di file che è possibile aprire (descrittori di file) per gli account utilizzati per la funzione dei servizi di Administration Server. A tale scopo, aprire il file /etc/security/limits.conf, quindi specificare i limiti soft e hard dei descrittori di file come segue:
   ```
   ksc     soft    nofile  32768
   ksc     hard    nofile  131072
   ```

4. Eseguire l'installazione di Kaspersky Security Center Linux. A seconda della distribuzione Linux, eseguire uno dei seguenti comandi:

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

5. Eseguire la configurazione di Kaspersky Security Center Linux:

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

6. Leggere il Contratto di licenza con l'utente finale (EULA) e l'Informativa sulla privacy. Il testo viene visualizzato nella finestra della riga di comando. Premere la barra spaziatrice per visualizzare il segmento di testo successivo. Quando richiesto inserire i seguenti valori:

   a. Immettere `y` se i termini del Contratto di licenza con l'utente finale sono stati compresi e accettati. Immettere `n` se non si accettano i termini del Contratto di licenza con l'utente finale. Per utilizzare Kaspersky Security Center Linux è necessario accettare i termini del Contratto di licenza con l'utente finale.

   b. Immettere `y` se i termini dell'Informativa sulla privacy sono stati compresi e accettati e se si accetta che i propri dati vengano gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy. Immettere `n` se non si accettano i termini dell'Informativa sulla privacy. Per utilizzare Kaspersky Security Center Linux è necessario accettare i termini dell'Informativa sulla privacy.

7. Quando richiesto, immettere le seguenti impostazioni:

   a. Immettere il nome DNS di Administration Server o l'indirizzo IP statico. Tale indirizzo verrà utilizzato da altri dispositivi per la connessione all'Administration Server.

   b. Immettere il numero di porta SSL di Administration Server. Per impostazione predefinita, viene utilizzata la porta 13000.

   c. Valutare il numero approssimativo di dispositivi che si intende gestire:

      - Se nella rete sono presenti da 1 a 100 dispositivi, immettere 1.
      - Se nella rete sono presenti da 101 a 1000 dispositivi, immettere 2.
      - Se nella rete sono presenti più di 1000 dispositivi, immettere 3.

   d. Immettere il nome del gruppo di protezione per i servizi. Per impostazione predefinita, viene utilizzato il gruppo "`kladmins`".

   e. Immettere il nome dell'account per avviare il servizio Administration Server. L'account deve essere un membro del gruppo di protezione inserito. Per impostazione predefinita, viene utilizzato l'account "`ksc`".

   f. Immettere il nome dell'account per avviare altri servizi. L'account deve essere un membro del gruppo di protezione inserito. Per impostazione predefinita, viene utilizzato l'account "`ksc`".

   g. Selezionare il DBMS installato per l'utilizzo con Kaspersky Security Center Linux:

      - Se è stato installato MySQL o MariaDB, immettere 1.
      - Se è stato installato PostgreSQL o Postgres Pro, immettere 2.

   h. Immettere il nome DNS o l'indirizzo IP del dispositivo in cui è installato il database. `127.0.0.1` per impostazione predefinita per un'installazione DB locale.

   i. Immettere il numero di porta del database. Questa porta viene utilizzata per comunicare con Administration Server. Per impostazione predefinita, vengono utilizzate le seguenti porte:

      - Porta `3306` per MySQL o MariaDB
      - Porta `5432` per PostgreSQL o Postgres Pro

j. Immettere il nome del database.

k. Immettere il nome utente dell'account radice del database utilizzato per accedere al database.

l. Immettere la password dell'account radice del database utilizzato per accedere al database.

Attendere che i servizi vengano aggiunti e avviati automaticamente:

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

m. Creare un account che fungerà da amministratore di Administration Server. Immettere il nome utente e la password. È possibile utilizzare il seguente comando per creare un nuovo utente:
`/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>`

La password deve rispettare le seguenti regole:

- La password utente non può contenere meno di 8 o più di 256 caratteri.
- La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
  - Lettere maiuscole (A-Z)
  - Lettere minuscole (a-z)
  - Numeri (0-9)
  - Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Viene aggiunto l'utente e viene installato Kaspersky Security Center Linux.

Verifica del servizio

Utilizzare i seguenti comandi per verificare se un servizio è in esecuzione o meno:

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Installazione di Kaspersky Security Center Linux in modalità automatica

È possibile installare Kaspersky Security Center Linux nei dispositivi Linux utilizzando un file di risposte per eseguire un'installazione in modalità automatica, ovvero senza la partecipazione dell'utente. Il file di risposte contiene un set personalizzato di parametri di installazione: variabili e rispettivi valori.

Prima dell'installazione:

- Installare un sistema di gestione database (DBMS).
- Verificare che il dispositivo in cui si desidera installare Kaspersky Security Center Linux esegua una delle distribuzioni Linux supportate.

Per installare Kaspersky Security Center Linux in modalità automatica:

1. Leggere il Contratto di licenza con l'utente finale. Seguire i passaggi di seguito solo se sono stati compresi e accettati i termini del Contratto di licenza con l'utente finale.
2. Se il dispositivo funziona con Astra Linux 1.8 o versione successiva, eseguire le azioni descritte in questo passaggio. Se il dispositivo viene eseguito su un sistema operativo diverso, procedere al passaggio successivo.

   a. Creare la directory /etc/systemd/system/kladminserver_srv.service.d e creare un file denominato override.conf con il seguente contenuto:
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klserver -d from_wd
   ```

   b. Creare una directory /etc/systemd/system/klwebsrv_srv.service.d e creare un file denominato override.conf con il seguente contenuto:
   ```
   [Service]
   User=
   User=ksc
   CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK
   ExecStart=
   ExecStart=/opt/kaspersky/ksc64/sbin/klcsweb -d from_wd
   ```

3. Creare un gruppo 'kladmins' e un account 'ksc' senza privilegi, che deve essere un membro del gruppo 'kladmins'. A tale scopo, eseguire in sequenza i seguenti comandi con un account con privilegi di root:
   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```
4. Creare il file di risposte (in formato TXT) e aggiungere un elenco di variabili nel formato `VARIABLE_NAME=variable_value` al file di risposte, ciascuna in una riga separata. Il file di risposte deve includere le variabili elencate nella tabella seguente.
5. Impostare il valore della variabile di ambiente `KLAUTOANSWERS` nell'ambiente radice o utente che contiene il nome completo del file di risposte (incluso il percorso), ad esempio con il seguente comando:
   ```
   export KLAUTOANSWERS=/tmp/ksc_install/answers.txt
   ```
6. Eseguire l'installazione di Kaspersky Security Center Linux in modalità automatica: a seconda della distribuzione Linux, eseguire uno dei seguenti comandi:

   Nell'ambiente radice:

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

   Nell'ambiente utente:

- `$ sudo -E apt install /<path>/ksc64_[ numero_versione ]_amd64.deb`
- `$ sudo -E yum install /<path>/ksc64-[ numero_versione ].x86_64.rpm -y`

7. Creare un utente per l'utilizzo di Kaspersky Security Center Web Console. A tale scopo, eseguire il seguente comando con un account con privilegi di root:

   `/opt/kaspersky/ksc64/sbin/kladduser -n ksc -p < password >`, dove la password deve contenere almeno 8 caratteri.

Variabili del file di risposte utilizzate come parametri dell'installazione di Kaspersky Security Center Linux in modalità automatica

Nome della variabile	Richiesto	Descrizione	Valori possibili
`EULA_ACCEPTED`	Sì	Conferma che l'utente ha compreso e accettato i termini del Contratto di licenza con l'utente finale.	`1`
`PP_ACCEPTED`	Sì	Conferma che l'utente ha compreso e accettato i termini dell'Informativa sulla privacy.	`1`
`KLSRV_UNATT_SERVERADDRESS`	Sì	Il nome DNS o l'indirizzo IP statico di Administration Server.	Nome DNS o indirizzo IP
`KLSRV_UNATT_PORT_SRV`	No	Il numero di porta di Administration Server. Facoltativamente, il valore predefinito è 14000.	Numero di porta
`KLSRV_UNATT_PORT_SRV_SSL`	No	Il numero di porta SSL di Administration Server. Facoltativamente, il valore predefinito è 13000.	Numero di porta
`KLSRV_UNATT_PORT_KLOAPI`	No	Il numero della porta per l'utilizzo di OpenAPI. Questa porta viene utilizzata anche per ricevere connessioni da Kaspersky Security Center Web Console. Facoltativamente, il valore predefinito è 13299.	Numero di porta
`KLSRV_UNATT_PORT_GUI`	No	Numero della porta per l'utilizzo dell'utilità klakaut. Facoltativamente, il valore predefinito è 13291. L'utilità klakaut e la relativa Guida sono disponibili nella cartella di installazione di Kaspersky Security Center Linux. Questa porta è chiusa per impostazione predefinita. Se si desidera utilizzare l'utilità klakaut per automatizzare il funzionamento di Kaspersky Security Center Linux, aprire la porta 13291 tramite l'utilità klscflag.	Numero di porta
`KLSRV_UNATT_NETRANGETYPE`	No	Il numero approssimativo di dispositivi che si intende gestire. Facoltativamente, il valore predefinito è 1.	`1` f1 per 1-100 dispositivi in rete. `2` per 101-1.000 dispositivi in rete. `3` per oltre 1.000 dispositivi in rete.
`KLSRV_UNATT_DBMS_INSTANCE`	Sì	L'indirizzo IP del server di database.	Indirizzo IP
`KLSRV_UNATT_DBMS_PORT`	Sì	La porta del server di database.	`3306`
`KLSRV_UNATT_DB_NAME`	Sì	Il nome del database.	`kav`
`KLSRV_UNATT_DBMS_LOGIN`	Sì	Il nome utente di un utente che ha accesso al database.	
`KLSRV_UNATT_DBMS_PASSWORD`	Sì	La password di un utente che ha accesso al database.	
`KLSRV_UNATT_KLADMINSGROUP`	Sì	Il nome del gruppo di protezione per i servizi.	`kladmins`
`KLSRV_UNATT_KLSRVUSER`	Sì	Il nome dell'account per avviare il servizio Administration Server. L'account deve essere un membro del gruppo di sicurezza specificato nella variabile `KLSRV_UNATT_KLADMINSGROUP`.	`ksc`
`KLSRV_UNATT_KLSVCUSER`	Sì	Il nome dell'account per avviare altri servizi.	`ksc`

		L'account deve essere un membro del gruppo di sicurezza specificato nella variabile `KLSRV_UNATT_KLADMINSGROUP`.	
Se Administration Server deve essere distribuito come cluster di failover Kaspersky Security Center Linux, il file di risposte deve includere le seguenti variabili aggiuntive:			

`KLFOC_UNATT_NODE`	Sì	Il numero del nodo (1 o 2).	`1`
			o
			`2`

`KLFOC_UNATT_STATE_SHARE_MOUNT_PATH`	Sì	Il punto di montaggio della condivisione degli stati.	
`KLFOC_UNATT_DATA_SHARE_MOUNT_PATH`	Sì	Il punto di montaggio della condivisione dei dati.	

`KLFOC_UNATT_CONN_MODE`	Sì	La modalità di connettività del cluster di failover.	`VirtualAdapter`
			o
			`ExternalLoadBalancer`

Nel caso in cui la variabile `KLFOC_UNATT_CONN_MODE` abbia un valore `VirtualAdapter`, il file di risposte deve includere le seguenti variabili aggiuntive:			
`KLFOC_UNATT_CONN_MODE_VA_NAME`	Sì	Il nome della scheda di rete virtuale.	
`KLFOC_UNATT_CONN_MODE_VA_IPV4`	Una di queste variabili è obbligatoria	L'indirizzo IP della scheda di rete virtuale.	Indirizzo IP
`KLFOC_UNATT_CONN_MODE_VA_IPV6`		L'indirizzo IPv6 della scheda di rete virtuale.	Indirizzo IPv6

Installazione di Kaspersky Security Center Linux su Astra Linux in modalità ambiente software chiuso

Questa sezione descrive come installare Kaspersky Security Center Linux nel sistema operativo Astra Linux Special Edition.

Prima dell'installazione:

- Installare il DBMS.
- Scaricare la chiave dell'applicazione kaspersky_astra_pub_key.gpg.

Utilizzare il file di installazione ksc64_[numero_versione]_amd64.deb. È possibile ottenere il file di installazione scaricandolo dal sito Web di Kaspersky.

In un account con privilegi di root, eseguire i comandi forniti in questa istruzione con integrità elevata e riservatezza zero.

Per installare Kaspersky Security Center Linux nel sistema operativo Astra Linux Special Edition (aggiornamento operativo 1.7.2) e Astra Linux Special Edition (aggiornamento operativo 1.6):

1. Aprire il file `/etc/digsig/digsig_initramfs.conf`, quindi specificare la seguente impostazione:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Nella riga di comando, eseguire il seguente comando per installare il pacchetto di compatibilità:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Creare una directory per la chiave dell'applicazione:

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

4. Posizionare la chiave dell'applicazione nella directory creata nel passaggio precedente:

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

5. Aggiornare l'immagine del file system RAM iniziale per tutti i kernel del sistema:

   ```
   update-initramfs -u -k all
   ```

   Riavviare il sistema.

6. Se il dispositivo funziona con Astra Linux 1.8 o versione successiva, eseguire le azioni descritte in questo passaggio. Se il dispositivo viene eseguito su un sistema operativo diverso, procedere al passaggio successivo.

   a. Creare la directory /etc/systemd/system/kladminserver_srv.service.d e creare un file denominato override.conf con il seguente contenuto:

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

   b. Creare una directory /etc/systemd/system/klwebsrv_srv.service.d e creare un file denominato override.conf con il seguente contenuto:

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

7. Creare un gruppo "kladmins" e un account "ksc" senza privilegi. L'account deve essere un membro del gruppo "kladmins". A tale scopo, eseguire in sequenza i seguenti comandi:

   ```
   # adduser ksc
   # groupadd kladmins
   # gpasswd -a ksc kladmins
   # usermod -g kladmins ksc
   ```

8. Eseguire l'installazione di Kaspersky Security Center Linux:

   ```
   # apt install /<percorso>/ksc64_[ numero_versione ]_amd64.deb
   ```

9. Eseguire la configurazione di Kaspersky Security Center Linux:

   ```
   # /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

10. Leggere il Contratto di licenza con l'utente finale (EULA) e l'Informativa sulla privacy. Il testo viene visualizzato nella finestra della riga di comando. Premere la barra spaziatrice per visualizzare il segmento di testo successivo. Quando richiesto, inserire i seguenti valori:

    a. Immettere `y` se i termini del Contratto di licenza con l'utente finale sono stati compresi e accettati. Immettere `n` se non si accettano i termini del Contratto di licenza con l'utente finale. Per utilizzare Kaspersky Security Center Linux è necessario accettare i termini del Contratto di licenza con l'utente finale.

    b. Immettere `y` se i termini dell'Informativa sulla privacy sono stati compresi e accettati e se si accetta che i propri dati vengano gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy. Immettere `n` se non si accettano i termini dell'Informativa sulla privacy. Per utilizzare Kaspersky Security Center Linux è necessario accettare i termini dell'Informativa sulla privacy.

11. Quando richiesto, immettere le seguenti impostazioni:

    a. Immettere il nome DNS di Administration Server o l'indirizzo IP statico.

    b. Immettere il numero di porta di Administration Server. Per impostazione predefinita, viene utilizzata la porta 14000.

    c. Immettere il numero di porta SSL di Administration Server. Per impostazione predefinita, viene utilizzata la porta 13000.

    d. Valutare il numero approssimativo di dispositivi che si intende gestire:

    - Se nella rete sono presenti da 1 a 100 dispositivi, immettere 1.
    - Se nella rete sono presenti da 101 a 1000 dispositivi, immettere 2.
    - Se nella rete sono presenti più di 1000 dispositivi, immettere 3.

    e. Immettere il nome del gruppo di protezione per i servizi. Per impostazione predefinita, viene utilizzato il gruppo "kladmins".

    f. Immettere il nome dell'account per avviare il servizio Administration Server. L'account deve essere un membro del gruppo di protezione inserito. Per impostazione predefinita, viene utilizzato l'account "ksc".

    g. Immettere il nome dell'account per avviare altri servizi. L'account deve essere un membro del gruppo di protezione inserito. Per impostazione predefinita, viene utilizzato l'account "ksc".

    h. Immettere l'indirizzo IP del dispositivo in cui è installato il database.

    i. Immettere il numero di porta del database. Questa porta viene utilizzata per comunicare con Administration Server. Per impostazione predefinita, viene utilizzata la porta 3306.

    j. Immettere il nome del database.

    k. Immettere il nome utente dell'account radice del database utilizzato per accedere al database.

    l. Immettere la password dell'account radice del database utilizzato per accedere al database.

    Attendere che i servizi vengano aggiunti e avviati automaticamente:

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

    m. Creare un account che fungerà da amministratore di Administration Server. Immettere il nome utente e la password.

    La password deve rispettare le seguenti regole:

    - La password utente deve avere un minimo di 8 e un massimo di 16 caratteri.
    - La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:

- Lettere maiuscole (A-Z)
- Lettere minuscole (a-z)
- Numeri (0-9)
- Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

Kaspersky Security Center Linux viene installato e l'utente viene aggiunto.

Verifica del servizio

Utilizzare i seguenti comandi per verificare se un servizio è in esecuzione o meno:

- `# systemctl status klnagent_srv.service`
- `# systemctl status kladminserver_srv.service`
- `# systemctl status klactprx_srv.service`
- `# systemctl status klwebsrv_srv.service`

Installazione di Kaspersky Security Center Web Console

Questa sezione descrive come installare Kaspersky Security Center Web Console Server (anche noto come Kaspersky Security Center Web Console) nei dispositivi che eseguono il sistema operativo Linux. Prima dell'installazione, è necessario installare un DBMS e Kaspersky Security Center Linux Administration Server.

Se si installa Kaspersky Security Center Web Console su Astra Linux in modalità ambiente software chiuso, seguire le istruzioni specifiche per Astra Linux.

Utilizzare uno dei seguenti file di installazione che corrisponde alla distribuzione Linux installata nel proprio dispositivo:

- Per Debian—ksc-web-console-[numero_build].x86_64.deb
- Per i sistemi operativi basati su RPM—ksc-web-console-[numero_build].x86_64.rpm
- Per ALT 8 SP—ksc-web-console-[numero_build]-alt8p.x86_64.rpm

È possibile ottenere il file di installazione scaricandolo dal sito Web di Kaspersky.

Per installare Kaspersky Security Center Web Console:

1. Verificare che il dispositivo in cui si desidera installare Kaspersky Security Center Web Console esegua una delle distribuzioni Linux supportate.
2. Leggere il Contratto di licenza con l'utente finale (EULA). Se il kit di distribuzione di Kaspersky Security Center Linux non include un file TXT con il testo dell'EULA, è possibile scaricare il file dal sito Web di Kaspersky. Se non si accettano le condizioni del Contratto di licenza, non installare l'applicazione.

3. Creare un file di risposta che contiene i parametri per la connessione di Kaspersky Security Center Web Console ad Administration Server. Denominare questo file ksc-web-console-setup.json e posizionarlo nella seguente directory: /etc/ksc-web-console-setup.json.

   Esempio di un file di risposta contenente il set minimo di parametri, nonché l'indirizzo e la porta predefiniti:

   ```
   {
     "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
   }
   ```

   È consigliabile specificare numeri di porta superiori a 1024. Se si desidera che Kaspersky Security Center Web Console funzioni sulle porte inferiori a 1024, dopo l'installazione è necessario eseguire il seguente comando:

   ```
   sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
   ```

   Quando si installa Kaspersky Security Center Web Console nel sistema operativo Linux ALT, è necessario specificare un numero di porta diverso da 8080, poiché la porta 8080 è utilizzata dal sistema operativo.

   Kaspersky Security Center Web Console non può essere aggiornato utilizzando lo stesso file di installazione .rpm. Se si desidera modificare le impostazioni in un file di risposta e utilizzare questo file per reinstallare l'applicazione, è prima necessario rimuovere l'applicazione, quindi reinstallarla con il nuovo file di risposta.

4. In un account con privilegi di root, utilizzare la riga di comando per eseguire il file di installazione con estensione .deb o .rpm, a seconda della distribuzione Linux.

   - Per installare o eseguire l'upgrade di Kaspersky Security Center Web Console da un file .deb, eseguire il comando seguente:
     ```
     $ sudo dpkg -i ksc-web-console-[numero_build].x86_64.deb
     ```
   - Per installare Kaspersky Security Center Web Console da un file .rpm, eseguire uno dei comandi seguenti:
     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-[numero_build].x86_64.rpm
     ```
     o
     ```
     $ sudo alien -i ksc-web-console-[numero_build].x86_64.rpm
     ```
   - Per eseguire l'upgrade da una versione precedente di Kaspersky Security Center Web Console, eseguire uno dei seguenti comandi:
     - Per i dispositivi che eseguono il sistema operativo basato su RPM:
       ```
       $ sudo rpm -Uvh --nodeps --force ksc-web-console-[numero_build].x86_64.rpm
       ```
     - Per i dispositivi che eseguono il sistema operativo basato su Debian:
       ```
       $ sudo dpkg -i ksc-web-console-[numero_build].x86_64.deb
       ```

   Verrà avviata la decompressione del file di installazione. Attendere il completamento dell'installazione. Kaspersky Security Center Web Console è installato nella seguente directory: /var/opt/kaspersky/ksc-web-console.

5. Riavviare tutti i servizi Kaspersky Security Center Web Console eseguendo il comando seguente:
   ```
   $ sudo systemctl restart KSC*
   ```

Al termine dell'installazione, è possibile utilizzare il browser per aprire e accedere a Kaspersky Security Center Web Console.

Parametri di installazione di Kaspersky Security Center Web Console

Per installare Kaspersky Security Center Web Console Server nei dispositivi che eseguono Linux, è necessario creare un file di risposta, ovvero un file .json che contiene i parametri per la connessione di Kaspersky Security Center Web Console ad Administration Server.

Ecco un esempio di un file di risposta contenente il set minimo di parametri, nonché l'indirizzo e la porta predefiniti:

```
{
  "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": "Group1:User2",
  "serviceWebConsoleAccount": "Group1:User3",
  "pluginAccount": "Group1:User4",
  "messageQueueAccount": "Group1:User5"
}
```

È consigliabile specificare numeri di porta superiori a 1024. Se si desidera che Kaspersky Security Center Web Console funzioni sulle porte inferiori a 1024, dopo l'installazione è necessario eseguire il seguente comando:

```
sudo setcap 'cap_net_bind_service=+ep' /var/opt/kaspersky/ksc-web-console/node
```

Quando si installa Kaspersky Security Center Web Console nel sistema operativo Linux ALT, è necessario specificare un numero di porta diverso da 8080, poiché la porta 8080 è utilizzata dal sistema operativo.

La tabella seguente descrive i parametri che possono essere specificati in un file di risposta.

Parametri per l'installazione di Kaspersky Security Center Web Console nei dispositivi che eseguono Linux

Parametro	Descrizione	Valori disponibili
`address`	Indirizzo di Kaspersky Security Center Web Console Server (obbligatorio).	Valore stringa.
`port`	Numero della porta utilizzata da Kaspersky Security Center Web Console Server per la connessione ad Administration Server (obbligatorio).	Valore numerico.
`defaultLangId`	Lingua dell'interfaccia utente (per impostazione predefinita, `1033`).	Codice numerico della lingua: • Tedesco: `1031` • Inglese: `1033` • Spagnolo: `3082` • Spagnolo (Messico): `2058` • Francese: `1036` • Giapponese: `1041`

		• Kazako: `1087` • Polacco: `1045` • Portoghese (Brasile): `1046` • Russo: `1049` • Turco: `1055` • Cinese semplificato: `4` • Cinese tradizionale: `31748` Se non viene specificato alcun valore, viene utilizzata la lingua inglese (en-US).
`enableLog`	Indica se abilitare o meno la registrazione delle attività di Kaspersky Security Center Web Console.	Valore booleano: • `true:` la registrazione è abilitata (selezionato per impostazione predefinita). • `false:` la registrazione è disabilitata.
`trusted`	Elenco degli Administration Server attendibili autorizzati a connettersi a Kaspersky Security Center Web Console. Ogni Administration Server deve essere definito con i seguenti parametri: • Indirizzo di Administration Server • Porta OpenAPI utilizzata da Kaspersky Security Center Web Console per la connessione ad Administration Server (per impostazione predefinita, 13299) • Percorso del certificato di Administration Server • Nome dell'Administration Server che verrà visualizzato nella finestra di accesso I parametri sono separati con barre verticali. Se vengono specificati più Administration Server, separarli con due barre verticali (pipe).	Valore stringa nel seguente formato: `" indirizzo server | porta | percorso certificato | nome server "`. Esempio: `"X.X.X.X|13299|/cert/server-1.cer| Server 1 ||Y.Y.Y.Y|13299|/cert/server-2.cer| Server 2 "`.
`acceptEula`	Indica se si desidera accettare o meno i termini del Contratto di licenza con l'utente finale (EULA). Il file contenente i termini del Contratto di licenza con l'utente finale viene scaricato insieme al file di installazione.	Valore booleano: • `true`: confermo di aver letto, compreso e accettato i termini e le condizioni del presente Contratto di licenza con l'utente finale. • `false`: non accetto i termini del Contratto di licenza (selezionato per impostazione predefinita). Se non viene specificato alcun valore, il programma di installazione di Kaspersky Security Center Web Console mostra l'EULA e chiede all'utente di accettarne o meno i termini.
`certDomain`	Se si desidera generare un nuovo certificato, utilizzare questo parametro per specificare il nome di dominio per cui deve essere generato un nuovo certificato.	Valore stringa.
`certPath`	Se si desidera utilizzare un certificato esistente, utilizzare questo parametro per specificare il percorso del file del certificato.	Valore stringa. Specificare il percorso `"/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"` per utilizzare il certificato esistente. Per un certificato personalizzato, specificare il relativo percorso di archiviazione.
`keyPath`	Se si desidera utilizzare un certificato esistente, utilizzare questo parametro per specificare il percorso del file della chiave.	Valore stringa.
`webConsoleAccount`	Nome dell'account con cui viene eseguito il servizio Kaspersky Security Center Web Console.	Valore stringa nel seguente formato: `" nome gruppo : nome utente "`. Esempio: `" Gruppo1 : Utente1 "`.

		Se non viene specificato alcun valore, il programma di installazione di Kaspersky Security Center Web Console crea un nuovo account con il nome predefinito `user_management_%uid%`.
`managementServiceAccount`	Nome dell'account privilegiato con cui viene eseguito Kaspersky Security Center Web Console Management Service.	Valore stringa nel seguente formato: `" nome gruppo : nome utente "`. Esempio: `" Gruppo1 : Utente1 "`. Se non viene specificato alcun valore, il programma di installazione di Kaspersky Security Center Web Console crea un nuovo account con il nome predefinito `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Nome dell'account con cui viene eseguito il servizio Kaspersky Security Center Web Console.	Valore stringa nel seguente formato: `" nome gruppo : nome utente "`. Esempio: `" Gruppo1 : Utente1 "`. Se non viene specificato alcun valore, il programma di installazione di Kaspersky Security Center Web Console crea un nuovo account con il nome predefinito `user_svc_nodejs_%uid%`.
`pluginAccount`	Nome dell'account con cui viene eseguito il servizio Kaspersky Security Center Product Plugins.	Valore stringa nel seguente formato: `" nome gruppo : nome utente "`. Esempio: `" Gruppo1 : Utente1 "`. Se non viene specificato alcun valore, il programma di installazione di Kaspersky Security Center Web Console crea un nuovo account con il nome predefinito `user_web_plugin_%uid%`.
`messageQueueAccount`	Nome dell'account con cui viene eseguito il servizio Kaspersky Security Center Web Console Message Queue.	Valore stringa nel seguente formato: `" nome gruppo : nome utente "`. Esempio: `" Gruppo1 : Utente1 "`. Se non viene specificato alcun valore, il programma di installazione di Kaspersky Security Center Web Console crea un nuovo account con il nome predefinito `user_message_queue_%uid%`.

Se vengono specificati i parametri `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` o `messageQueueAccount`, assicurarsi che gli account utente personalizzati appartengano allo stesso gruppo di protezione. Se questi parametri non vengono specificati, il programma di installazione di Kaspersky Security Center Web Console crea un gruppo di protezione predefinito, quindi crea account utente con nomi predefiniti in questo gruppo.

Installazione di Kaspersky Security Center Web Console su Astra Linux in modalità ambiente software chiuso

Questa sezione descrive come installare Kaspersky Security Center Web Console Server (anche noto come Kaspersky Security Center Web Console) nel sistema operativo Astra Linux Special Edition. Prima dell'installazione, è necessario installare un DBMS e Kaspersky Security Center Linux Administration Server.

Per installare Kaspersky Security Center Web Console:

1. Verificare che il dispositivo in cui si desidera installare Kaspersky Security Center Web Console esegua una delle distribuzioni Linux supportate.

2. Leggere il Contratto di licenza con l'utente finale (EULA). Se il kit di distribuzione di Kaspersky Security Center Linux non include un file TXT con il testo dell'EULA, è possibile scaricare il file dal sito Web di Kaspersky. Se non si accettano le condizioni del Contratto di licenza, non installare l'applicazione.

3. Creare un file di risposta che contiene i parametri per la connessione di Kaspersky Security Center Web Console ad Administration Server. Denominare questo file ksc-web-console-setup.json e posizionarlo nella seguente directory: /etc/ksc-web-console-setup.json.

Esempio di un file di risposta contenente il set minimo di parametri, nonché l'indirizzo e la porta predefiniti:

```
{
  "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. Aprire il file `/etc/digsig/digsig_initramfs.conf`, quindi specificare la seguente impostazione:

   ```
   DIGSIG_ELF_MODE=1
   ```

5. Nella riga di comando, eseguire il seguente comando per installare il pacchetto di compatibilità:

   ```
   apt install astra-digsig-oldkeys
   ```

6. Creare una directory per la chiave dell'applicazione:

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

7. Posizionare la chiave dell'applicazione `/opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg` nella directory creata nel passaggio precedente:

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

   Se il kit di distribuzione di Kaspersky Security Center Linux non include la chiave dell'applicazione kaspersky_astra_pub_key.gpg, è possibile scaricarla facendo clic sul collegamento: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Aggiornare i dischi RAM:

   ```
   update-initramfs -u -k all
   ```

   Riavviare il sistema.

9. In un account con privilegi di root, utilizzare la riga di comando per eseguire il file di installazione. È possibile ottenere il file di installazione scaricandolo dal sito Web di Kaspersky.

   - Per installare o eseguire l'upgrade di Kaspersky Security Center Web Console, eseguire il comando seguente:

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

   - Per eseguire l'upgrade da una versione precedente di Kaspersky Security Center Web Console, eseguire il comando seguente:

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

   Verrà avviata la decompressione del file di installazione. Attendere il completamento dell'installazione. Kaspersky Security Center Web Console è installato nella seguente directory: `/var/opt/kaspersky/ksc-web-console`.

10. Riavviare tutti i servizi Kaspersky Security Center Web Console eseguendo il comando seguente:

    ```
    $ sudo systemctl restart KSC*
    ```

Al termine dell'installazione, è possibile utilizzare il browser per aprire e accedere a Kaspersky Security Center Web Console.

Se il dispositivo funziona con Astra Linux 1.8, è necessario sovrascrivere i diritti utente dopo l'installazione di Kaspersky Security Center Web Console.

Si consiglia di eseguire separatamente i passaggi delle istruzioni per ciascun servizio.

Per sovrascrivere i diritti utente:

1. Aprire i seguenti file:
   - /etc/systemd/system/ KSCSvcWebConsole.service
   - /etc/systemd/system/ KSCWebConsole.service
   - /etc/systemd/system/ KSCWebConsoleManagement.service
   - /etc/systemd/system/ KSCWebConsoleMessageQueue.service
   - /etc/systemd/system/ KSCWebConsolePlugin.service
2. Copiare la stringa `User= valore` dai file.

   I valori sono diversi per ogni servizio e vengono generati durante l'installazione di Kaspersky Security Center Web Console.
3. Creare le seguenti directory:
   - /etc/systemd/system/ KSCSvcWebConsole.service.d
   - /etc/systemd/system/ KSCWebConsole.service.d
   - /etc/systemd/system/ KSCWebConsoleManagement.service.d
   - /etc/systemd/system/ KSCWebConsoleMessageQueue.service.d
   - /etc/systemd/system/ KSCWebConsolePlugin.service.d
4. In ogni directory creare un file denominato `override.conf`, quindi inserire la stringa copiata al passaggio 2 nel file. Il file `override.conf` deve avere il seguente contenuto:
   - per **/etc/systemd/system/ KSCSvcWebConsole.service.d**

     ```
     [Service]

     User=

     User= valore

     CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK

     ExecStart=

     ExecStart=/usr/bin/env /var/opt/kaspersky/ksc-web-console/node
     /var/opt/kaspersky/ksc-web-console/pm.service-console.js
     ```

- per /etc/systemd/system/ KSCWebConsole.service.d

```
[Service]

User=

User= valore

CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK

ExecStart=

ExecStart=/usr/bin/env /var/opt/kaspersky/ksc-web-console/node
/var/opt/kaspersky/ksc-web-console/pm.js
```

- per /etc/systemd/system/ KSCWebConsoleManagement.service.d

```
[Service]

User=

User= valore

CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK

ExecStart=

ExecStart=/usr/bin/env /var/opt/kaspersky/ksc-web-console/node
/var/opt/kaspersky/ksc-web-console/pm.updates-manager.js
```

- per /etc/systemd/system/ KSCWebConsoleMessageQueue.service.d

```
[Service]

User=

User= valore

CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK

ExecStart=

ExecStart=/usr/bin/env /var/opt/kaspersky/ksc-web-console/vendor/nsqd -tls-
cert=../nsq-server.crt -tls-key=../nsq-server.key -tls-required=1 -tls-min-
version=tls1.2 -tls-root-ca-file=../KLRootCA.crt -max-msg-size=10485760 -mem-
queue-size=100 -sync-every=0 -sync-timeout=24h -http-address=127.0.0.1:4151 -
https-address=127.0.0.1:4152 -tcp-address=127.0.0.1:4150 -tls-client-auth-
policy=require-verify
```

- per /etc/systemd/system/ KSCWebConsolePlugin.service.d

```
[Service]

User=

User= valore

CapabilitiesParsec=PARSEC_CAP_PRIV_SOCK

ExecStart=

ExecStart=/usr/bin/env /var/opt/kaspersky/ksc-web-console/node
/var/opt/kaspersky/ksc-web-console/pm.plugin.js
```

dove `User= valore` è la stringa copiata nel passaggio 2. Ad esempio, `User=user_svc_nodejs_rjvyyf-xkg`.

5. Riavviare il servizio.

Installazione di Kaspersky Security Center Web Console connesso all'Administration Server installato nei nodi del cluster di failover Kaspersky Security Center Linux

Questa sezione descrive come installare Kaspersky Security Center Web Console Server (di seguito anche Kaspersky Security Center Web Console), che si connette all'Administration Server installato nei nodi del cluster di failover Kaspersky Security Center Linux. Prima di installare Kaspersky Security Center Web Console, installare un DBMS e Kaspersky Security Center Linux Administration Server nei nodi del cluster di failover Kaspersky Security Center Linux.

Kaspersky Security Center Web Console non supporta il clustering. Si consiglia di installare Kaspersky Security Center Web Console su un server separato.

Per installare Kaspersky Security Center Web Console che si connette all'Administration Server installato nei nodi del cluster di failover Kaspersky Security Center Linux:

1. Eseguire il passaggio 1 e il passaggio 2 dell'installazione di Kaspersky Security Center Web Console.

2. Al passaggio 3, nel file di risposta, specificare il parametro di installazione `attendibile` per consentire a Kaspersky Security Center Web Console di connettersi al cluster di failover di Kaspersky Security Center Linux. Il valore stringa di questo parametro ha il seguente formato:
   `"trusted": "indirizzo server|porta|percorso certificato|nome server"`

   Specificare i componenti del parametro di installazione `trusted`:

   - **Indirizzo di Administration Server**. Se una scheda di rete secondaria è stata creata durante la preparazione dei nodi del cluster, utilizzare l'indirizzo IP della scheda come indirizzo del cluster di failover Kaspersky Security Center Linux. In caso contrario, specificare l'indirizzo IP del sistema di bilanciamento del carico di terzi in uso.

   - **Porta di Administration Server**. La porta OpenAPI utilizzata da Kaspersky Security Center Web Console per la connessione ad Administration Server (il valore predefinito è 13299).

- **Certificato di Administration Server**. Il certificato di Administration Server si trova nell'archivio dati condiviso del cluster di failover Kaspersky Security Center Linux. Il percorso predefinito del file del certificato: <cartella dati condivisa> \1093\cert\klserver.cer. Copiare il file del certificato dall'archivio dati condiviso nel dispositivo in cui si installa Kaspersky Security Center Web Console. Specificare il percorso locale del certificato di Administration Server.

- **Nome Administration Server**. Il nome del cluster di failover Kaspersky Security Center Linux che verrà visualizzato nella finestra di accesso di Kaspersky Security Center Web Console.

3. Continuare con l'installazione standard di Kaspersky Security Center Web Console.

Al termine dell'installazione, sul desktop viene visualizzato un collegamento ed è possibile accedere a Kaspersky Security Center Web Console.

Distribuzione del cluster di failover Kaspersky Security Center Linux

Questa sezione contiene sia informazioni generali sul cluster di failover Kaspersky Security Center Linux che istruzioni sulla preparazione e sulla distribuzione del cluster di failover Kaspersky Security Center Linux nella rete.

Scenario: Distribuzione di un cluster di failover Kaspersky Security Center Linux

Un cluster di failover Kaspersky Security Center Linux garantisce un'elevata disponibilità di Kaspersky Security Center Linux e riduce al minimo i tempi di inattività di Administration Server in caso di errore. Il cluster di failover si basa su due istanze identiche di Kaspersky Security Center Linux installate in due computer. Una delle istanze funge da nodo attivo e l'altra da nodo passivo. Il nodo attivo gestisce la protezione dei dispositivi client, mentre quello passivo è predisposto a svolgere tutte le funzioni del nodo attivo in caso di errore del nodo attivo. Quando si verifica un errore, il nodo passivo diventa attivo e il nodo attivo diventa passivo.

Prerequisiti

È necessario disporre dell'hardware che soddisfi i requisiti per il cluster di failover.

La distribuzione delle applicazioni Kaspersky prevede diversi passaggi:

1. **Preparazione del file server**

   Preparare il file server affinché funzioni come componente del cluster di failover Kaspersky Security Center Linux. Assicurarsi che il file server soddisfi i requisiti hardware e software, creare due cartelle condivise per i dati di Kaspersky Security Center Linux e configurare le autorizzazioni per accedere alle cartelle condivise.

   Istruzioni dettagliate: Preparazione di un file server per il cluster di failover Kaspersky Security Center Linux

2. **Preparazione di nodi attivi e passivi**

   Preparare due dispositivi con hardware e software identici in modo che fungano da nodi attivi e passivi.

   Istruzioni dettagliate: Preparazione dei nodi per il cluster di failover Kaspersky Security Center Linux

3. **Creazione di account per i servizi di Kaspersky Security Center Linux**

   Effettuare le seguenti operazioni sul nodo attivo, sul nodo passivo e sul file server:

   1. Creare un gruppo con il nome "kladmins" e assegnare lo stesso GID a tutti e tre i gruppi.

2. Creare un account utente con il nome "ksc" e assegnare lo stesso UID a tutti e tre gli account utente. Impostare il gruppo primario su "kladmins" per gli account creati.

3. Creare un account utente con il nome "rightless" e assegnare lo stesso UID a tutti e tre gli account utente. Impostare il gruppo primario su "kladmins" per gli account creati.

4. **Installazione del DBMS (Database Management System)**

   Sono disponibili due opzioni:

   - Se si desidera utilizzare MariaDB Galera Cluster, non è necessario un dispositivo dedicato per DBMS. Installare MariaDB Galera Cluster in ciascuno dei nodi.
   - Se si desidera usare qualsiasi altro DBMS supportato, installare il DBMS selezionato in un dispositivo dedicato.

5. **Installazione di Kaspersky Security Center Linux**

   Installare Kaspersky Security Center Linux in modalità cluster di failover in entrambi i nodi. È prima necessario installare Kaspersky Security Center Linux nel nodo attivo, quindi installarlo in quello passivo.

   Inoltre, è possibile installare Kaspersky Security Center Web Console in un dispositivo separato che non sia un nodo del cluster.

6. **Test del cluster di failover**

   Verificare di aver configurato correttamente il cluster di failover e che funzioni correttamente. È ad esempio possibile arrestare uno dei servizi di Kaspersky Security Center Linux nel nodo attivo: kladminserver, klnagent, ksnproxy, klactprx o klwebsrv. Dopo l'arresto del servizio, la gestione della protezione deve passare automaticamente al nodo passivo.

Risultati

Il cluster di failover Kaspersky Security Center Linux viene distribuito. Familiarizzare con gli eventi che determinano il passaggio dai nodi attivi a quelli passivi.

Informazioni sul cluster di failover Kaspersky Security Center Linux

Un cluster di failover Kaspersky Security Center Linux garantisce un'elevata disponibilità di Kaspersky Security Center Linux e riduce al minimo i tempi di inattività di Administration Server in caso di errore. Il cluster di failover si basa su due istanze identiche di Kaspersky Security Center Linux installate in due computer. Una delle istanze funge da nodo attivo e l'altra da nodo passivo. Il nodo attivo gestisce la protezione dei dispositivi client, mentre quello passivo è predisposto a svolgere tutte le funzioni del nodo attivo in caso di errore del nodo attivo. Quando si verifica un errore, il nodo passivo diventa attivo e il nodo attivo diventa passivo.

> In un cluster di failover Kaspersky Security Center Linux, tutti i servizi di Kaspersky Security Center Linux vengono gestiti automaticamente. Non tentare di riavviare i servizi manualmente.

Requisiti hardware e software

Per distribuire un cluster di failover Kaspersky Security Center Linux, è necessario disporre del seguente hardware:

- Due dispositivi con hardware e software identici. Questi dispositivi fungeranno da nodi attivi e passivi.

- Un file server che esegue Linux, con il file system EXT4. È necessario mettere a disposizione un dispositivo dedicato che fungerà da file server.

  Assicurarsi di aver fornito un'elevata larghezza di banda di rete tra il file server e i nodi attivi e passivi.

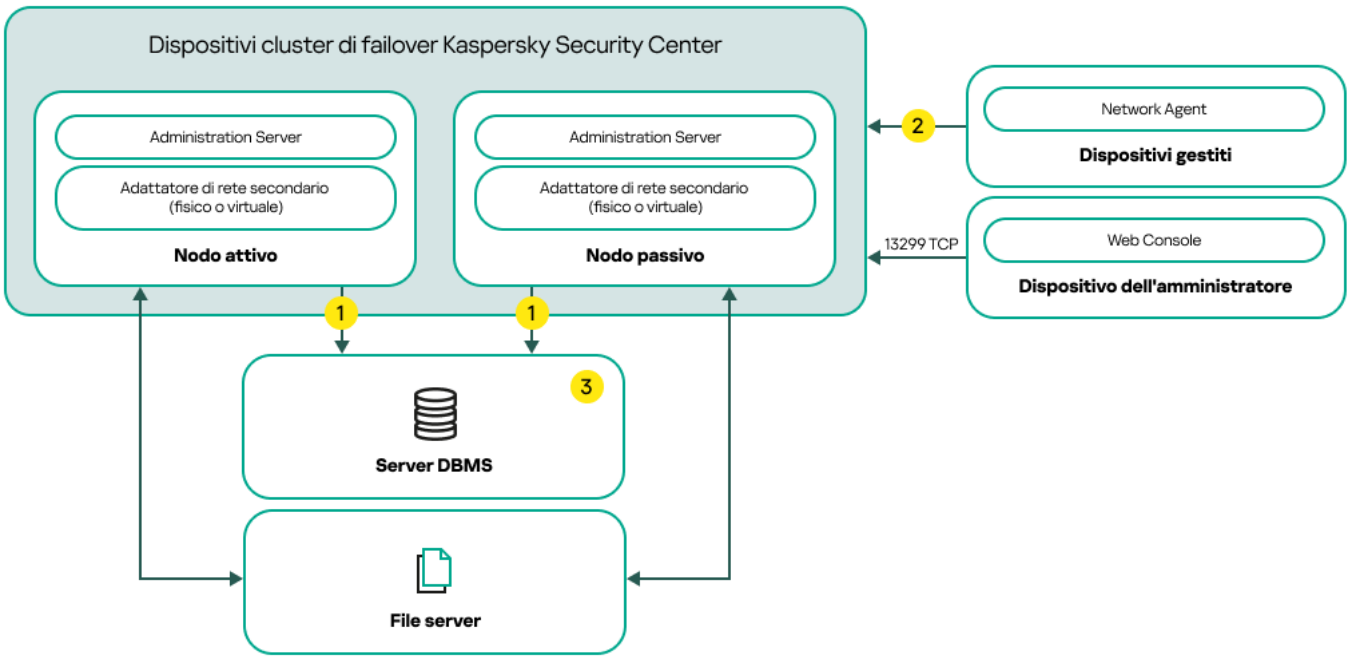
- Un dispositivo con DBMS (Database Management System) supportato. Se si utilizza MariaDB Galera Cluster come DBMS, non è necessario un dispositivo dedicato per questo scopo.

L'implementazione del cluster di failover fallisce quando sono installati entrambi i pacchetti arping e iputils-arping oppure solo il pacchetto arping. Prima di distribuire un cluster di failover, assicurarsi di avere installato solo il pacchetto di installazione iputils-arping su entrambi i nodi.

Schemi di distribuzione

È possibile scegliere uno dei seguenti schemi per distribuire il cluster di failover Kaspersky Security Center Linux:

- Uno schema che utilizza una scheda di rete secondaria.
- Uno schema che utilizza un sistema di bilanciamento del carico di terze parti.



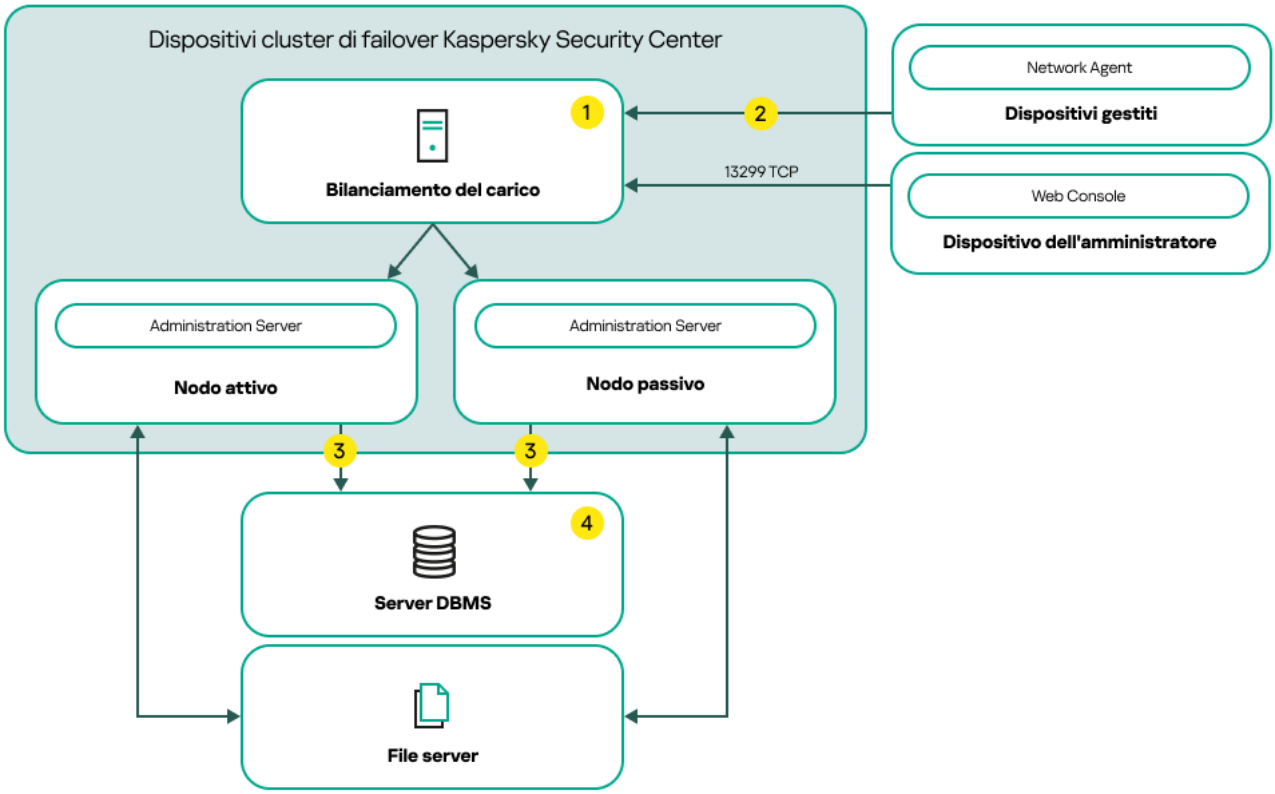
Uno schema che utilizza una scheda di rete secondaria

Legenda schema:

1 Administration Server invia i dati al database. Aprire le porte necessarie nel dispositivo in cui si trova il database, ad esempio la porta 3306 per MySQL Server o la porta 5432 per PostgreSQL o Postgres Pro. Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2 Nei dispositivi gestiti aprire le seguenti porte: TCP 13000, UDP 13000 e TCP 17000.

3 Un dispositivo con DBMS (Database Management System). Se si utilizza MariaDB Galera Cluster come DBMS, non è necessario un dispositivo dedicato per questo scopo. Installare MariaDB Galera Cluster in ciascuno dei nodi.



Uno schema che utilizza un sistema di bilanciamento del carico di terze parti

Legenda schema:

1 Nel dispositivo di bilanciamento del carico aprire tutte le porte di Administration Server: TCP 13000, UDP 13000, TCP 13299 e TCP 17000.

> Se si desidera utilizzare l'utilità klakaut per l'automazione, è necessario aprire anche la porta TCP 13291.

2 Nei dispositivi gestiti aprire le seguenti porte: TCP 13000, UDP 13000 e TCP 17000.

3 Administration Server invia i dati al database. Aprire le porte necessarie nel dispositivo in cui si trova il database, ad esempio la porta 3306 per MySQL Server o la porta 5432 per PostgreSQL o Postgres Pro. Fare riferimento alla documentazione DBMS per le informazioni attinenti.

4 Un dispositivo con DBMS (Database Management System). Se si utilizza MariaDB Galera Cluster come DBMS, non è necessario un dispositivo dedicato per questo scopo. Installare MariaDB Galera Cluster in ciascuno dei nodi.

Condizioni per il passaggio

Il cluster di failover passa la gestione della protezione dei dispositivi client dal nodo attivo a quello passivo se si verifica uno dei seguenti eventi nel nodo attivo:

- Il nodo attivo è danneggiato a causa di un errore software o hardware.
- Il nodo attivo è stato temporaneamente arrestato per attività di manutenzione.
- Almeno uno dei servizi (o processi) di Kaspersky Security Center Linux non è riuscito o è stato deliberatamente terminato dall'utente. I servizi di Kaspersky Security Center Linux sono i seguenti: kladminserver, klnagent, klactprx e klwebsrv.

- La connessione di rete tra il nodo attivo e l'archivio nel file server è stata interrotta o terminata.

Preparazione di un file server per un cluster di failover Kaspersky Security Center Linux

Un file server funge da componente necessario di un cluster di failover Kaspersky Security Center Linux.

Per preparare un file server:

1. Assicurarsi che il file server soddisfi i requisiti hardware e software.
2. Installare e configurare un server NFS:
   - L'accesso al file server deve essere abilitato per entrambi i nodi nelle impostazioni del server NFS.
   - Il protocollo NFS deve avere la versione 4.0 o 4.1.
   - Requisiti minimi per il kernel Linux:
     - 3.19.0-25, se si utilizza NFS 4.0
     - 4.4.0-176, se si utilizza NFS 4.1
3. Nel file server, creare due cartelle e condividerle utilizzando NFS. Una di queste verrà utilizzata per conservare le informazioni sullo stato del cluster di failover. L'altra verrà utilizzata per archiviare i dati e le impostazioni di Kaspersky Security Center Linux. Specificare i percorsi delle cartelle condivise durante la configurazione dell'installazione di Kaspersky Security Center Linux.

   A seconda della distribuzione Linux, installare il pacchetto nfs-utils o il pacchetto nfs-kernel-server eseguendo il comando corrispondente:

   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

   Eseguire i seguenti comandi:

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

   Abilitare l'avvio automatico eseguendo il comando seguente:

   ```
   sudo systemctl enable rpcbind
   ```

4. Riavviare il file server.

Il file server è pronto. Per distribuire il cluster di failover Kaspersky Security Center Linux, seguire le istruzioni aggiuntive in questo scenario.

Preparazione dei nodi per un cluster di failover Kaspersky Security Center Linux

Preparare due dispositivi affinché fungano da nodi attivi e passivi del cluster di failover Kaspersky Security Center Linux.

Per preparare i nodi per il cluster di failover Kaspersky Security Center Linux:

1. Assicurarsi di avere due dispositivi che soddisfino i requisiti hardware e software. Questi dispositivi fungeranno da nodi attivi e passivi del cluster di failover.

2. A seconda della distribuzione Linux, installare il pacchetto nfs-utils o il pacchetto nfs-kernel-server in ciascun nodo eseguendo il comando corrispondente:
   ```
   sudo yum install nfs-utils
   sudo apt install nfs-kernel-server
   ```

3. Creare i punti di montaggio eseguendo i seguenti comandi:
   ```
   sudo mkdir -p /mnt/KlFocStateShare
   sudo mkdir -p /mnt/KlFocDataShare_klfoc
   ```

4. Abbinare i punti di montaggio e le cartelle condivise:
   ```
   sudo sh -c "echo {server}:{path to the KlFocStateShare folder} /mnt/KlFocStateShare
   nfs vers=4,soft,timeo=50,retrans=2,auto,user,rw 0 0 >> /etc/fstab"
   sudo sh -c "echo {server}:{percorso della cartella KlFocDataShare_klfoc}
   /mnt/KlFocDataShare_klfoc nfs vers=4,noauto,user,rw,exec 0 0 >> /etc/fstab"
   ```
   Qui, `{server}:{percorso della cartella KlFocStateShare}` e `{server}:{percorso della cartella KlFocDataShare_klfoc}` sono i percorsi di rete delle cartelle condivise nel file server.

5. Montare le cartelle condivise eseguendo i seguenti comandi:
   ```
   mount /mnt/KlFocStateShare
   mount /mnt/KlFocDataShare_klfoc
   ```

6. Assicurarsi che le autorizzazioni per accedere alle cartelle condivise appartengano a ksc:kladmins.

   Eseguire il seguente comando:
   ```
   sudo ls -la /mnt/
   ```

7. In ogni nodo, configurare una scheda di rete secondaria.

   Una scheda di rete secondaria può essere fisica o virtuale. Se si desidera utilizzare una scheda di rete fisica, connetterla e configurarla con gli strumenti standard del sistema operativo. Se si desidera utilizzare una scheda di rete virtuale, crearla utilizzando software di terzi.

   Eseguire una delle seguenti operazioni:

   - Utilizzare una scheda di rete virtuale.

     a. Utilizzare il seguente comando per verificare che venga utilizzato NetworkManager per gestire la scheda fisica:
        ```
        nmcli device status
        ```

        Se la scheda fisica viene mostrata come non gestita nell'output, configurare NetworkManager in modo che gestisca la scheda fisica. Gli esatti passaggi di configurazione dipendono dalla distribuzione effettiva.

     b. Utilizzare il seguente comando per identificare le interfacce:

```
ip a
```

c. Creare un nuovo profilo di configurazione:

```
nmcli connection add type macvlan dev <interfaccia fisica> mode bridge
ifname <interfaccia virtuale> ipv4.addresses <maschera indirizzo>
ipv4.method manual autoconnect no
```

- Utilizzare una scheda di rete fisica o un hypervisor. In questo caso, disabilitare il software NetworkManager.

a. Eliminare le connessioni di NetworkManager per l'interfaccia di destinazione:

```
nmcli con del <nome connessione>
```

Utilizzare il seguente comando per verificare se l'interfaccia di destinazione dispone di connessioni:

```
nmcli con show
```

b. Modificare il file NetworkManager.conf. Individuare la sezione keyfile e assegnare l'interfaccia di destinazione al parametro dei dispositivi non gestiti.

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

c. Riavviare NetworkManager:

```
systemctl reload NetworkManager
```

Utilizzare il seguente comando per verificare che l'interfaccia di destinazione non sia gestita:

```
nmcli dev status
```

- Utilizzare un sistema di bilanciamento del carico di terze parti. È ad esempio possibile utilizzare un server nginx. In questo caso, procedere come segue:

a. Mettere a disposizione un dispositivo basato su Linux dedicato con nginx installato.

b. Configurare il bilanciamento del carico. Impostare il nodo attivo come server principale e il nodo passivo come server di backup.

c. Nel server nginx aprire tutte le porte di Administration Server: TCP 13000, UDP 13000, TCP 13299, TCP 17000.

> Se si desidera utilizzare l'utilità klakaut per l'automazione, è necessario aprire anche la porta TCP 13291.

I nodi sono pronti. Per distribuire il cluster di failover Kaspersky Security Center Linux, seguire le istruzioni aggiuntive dello scenario.

Installazione di Kaspersky Security Center Linux nei nodi del cluster di failover Kaspersky Security Center Linux

Questa procedura descrive come installare Kaspersky Security Center Linux nei nodi del cluster di failover Kaspersky Security Center Linux. Kaspersky Security Center Linux viene installato separatamente in entrambi i nodi del cluster di failover Kaspersky Security Center Linux. Prima si installa l'applicazione nel nodo attivo, poi su quello passivo. Durante l'installazione, è necessario scegliere quale nodo sarà attivo e quale sarà passivo.

Usare il file di installazione—ksc64_[numero_versione]_amd64.deb or ksc64-[numero_versione].x86_64.rpm—che corrisponde alla distribuzione Linux installata nel dispositivo. È possibile ottenere il file di installazione scaricandolo dal sito Web di Kaspersky.

Installazione nel nodo primario (attivo)

Per installare Kaspersky Security Center Linux nel nodo primario:

1. Verificare che il dispositivo in cui si desidera installare Kaspersky Security Center Linux esegua una delle distribuzioni Linux supportate.

2. Nella riga di comando, eseguire i comandi forniti in questa istruzione.

3. Eseguire l'installazione di Kaspersky Security Center Linux. A seconda della distribuzione Linux, eseguire uno dei seguenti comandi:

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

4. Eseguire la configurazione di Kaspersky Security Center Linux:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Leggere il Contratto di licenza con l'utente finale (EULA) e l'Informativa sulla privacy. Il testo viene visualizzato nella finestra della riga di comando. Premere la barra spaziatrice per visualizzare il segmento di testo successivo. Quando richiesto inserire i seguenti valori:

   a. Immettere `y` se i termini del Contratto di licenza con l'utente finale sono stati compresi e accettati. Immettere `n` se non si accettano i termini del Contratto di licenza con l'utente finale. Per utilizzare Kaspersky Security Center Linux è necessario accettare i termini del Contratto di licenza con l'utente finale.

   b. Immettere `y` se i termini dell'Informativa sulla privacy sono stati compresi e accettati e se si accetta che i propri dati vengano gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy. Immettere `n` se non si accettano i termini dell'Informativa sulla privacy. Per utilizzare Kaspersky Security Center Linux è necessario accettare i termini dell'Informativa sulla privacy.

6. Selezionare **Nodo cluster primario** come modalità di installazione di Administration Server.

7. Quando richiesto, immettere le seguenti impostazioni:

   a. Immettere il percorso locale del punto di montaggio della condivisione degli stati.

   b. Immettere il percorso locale del punto di montaggio della condivisione dei dati.

   c. Scegliere una modalità di connettività del cluster di failover: tramite una scheda di rete secondaria o un servizio di bilanciamento del carico esterno.

   d. Se si utilizza una scheda di rete secondaria, immetterne il nome.

   e. Quando viene richiesto di immettere il nome DNS o l'indirizzo IP statico di Administration Server, immettere l'indirizzo IP della scheda di rete secondaria o l'indirizzo IP del servizio di bilanciamento del carico esterno.

   f. Immettere il numero di porta SSL di Administration Server. Per impostazione predefinita, viene utilizzata la porta 13000.

g. Valutare il numero approssimativo di dispositivi che si intende gestire:

- Se nella rete sono presenti da 1 a 100 dispositivi, immettere 1.
- Se nella rete sono presenti da 101 a 1000 dispositivi, immettere 2.
- Se nella rete sono presenti più di 1000 dispositivi, immettere 3.

h. Immettere il nome del gruppo di protezione per i servizi. Per impostazione predefinita, viene utilizzato il gruppo kladmins.

i. Immettere il nome dell'account per avviare il servizio Administration Server. L'account deve essere un membro del gruppo di protezione inserito. Per impostazione predefinita, viene utilizzato l'account "ksc".

j. Immettere il nome dell'account per avviare altri servizi. L'account deve essere un membro del gruppo di protezione inserito. Per impostazione predefinita, viene utilizzato l'account "ksc".

k. Selezionare il DBMS installato per l'utilizzo con Kaspersky Security Center Linux:

- Se è stato installato MySQL o MariaDB, immettere 1.
- Se è stato installato PostgreSQL o Postgres Pro, immettere 2.

l. Immettere il nome DNS o l'indirizzo IP del dispositivo in cui è installato il database.

m. Immettere il numero di porta del database. Questa porta viene utilizzata per comunicare con Administration Server. Per impostazione predefinita, vengono utilizzate le seguenti porte:

- Porta 3306 per MySQL o MariaDB
- Porta 5432 per PostgreSQL o Postgres Pro

n. Immettere il nome del database.

o. Immettere il nome utente dell'account radice del database utilizzato per accedere al database.

p. Immettere la password dell'account radice del database utilizzato per accedere al database.

8. Attendere che i servizi vengano aggiunti e avviati automaticamente:

- klfocsvc_klfoc
- kladminserver_klfoc
- klwebsrv_klfoc
- klactprx_klfoc
- klnagent_klfoc

9. Creare un account che fungerà da amministratore di Administration Server. Immettere il nome utente e la password. La password utente non può contenere meno di 8 o più di 16 caratteri.

Viene aggiunto l'utente e viene installato Kaspersky Security Center Linux nel nodo primario.

Installazione nel nodo secondario (passivo)

Per installare Kaspersky Security Center Linux nel nodo secondario:

1. Verificare che il dispositivo in cui si desidera installare Kaspersky Security Center Linux esegua una delle distribuzioni Linux supportate.

2. Nella riga di comando, eseguire i comandi forniti in questa istruzione.

3. Eseguire l'installazione di Kaspersky Security Center Linux. A seconda della distribuzione Linux, eseguire uno dei seguenti comandi:

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

4. Eseguire la configurazione di Kaspersky Security Center Linux:

   ```
   sudo /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl
   ```

5. Leggere il Contratto di licenza con l'utente finale (EULA) e l'Informativa sulla privacy. Il testo viene visualizzato nella finestra della riga di comando. Premere la barra spaziatrice per visualizzare il segmento di testo successivo. Quando richiesto inserire i seguenti valori:

   a. Immettere `y` se i termini del Contratto di licenza con l'utente finale sono stati compresi e accettati. Immettere `n` se non si accettano i termini del Contratto di licenza con l'utente finale. Per utilizzare Kaspersky Security Center Linux è necessario accettare i termini del Contratto di licenza con l'utente finale.

   b. Immettere `y` se i termini dell'Informativa sulla privacy sono stati compresi e accettati e se si accetta che i propri dati vengano gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy. Immettere `n` se non si accettano i termini dell'Informativa sulla privacy. Per utilizzare Kaspersky Security Center Linux è necessario accettare i termini dell'Informativa sulla privacy.

6. Selezionare **Nodo cluster secondario** come modalità di installazione di Administration Server.

7. Quando richiesto, immettere il percorso locale del punto di montaggio della condivisione degli stati.

Kaspersky Security Center Linux viene installato nel nodo secondario.

Verifica del servizio

Utilizzare i seguenti comandi per verificare se un servizio è in esecuzione o meno:

- `systemctl status klnagent_srv.service`
- `systemctl status kladminserver_srv.service`
- `systemctl status klactprx_srv.service`
- `systemctl status klwebsrv_srv.service`

Adesso è possibile testare il cluster di failover Kaspersky Security Center Linux per assicurarsi di averlo configurato correttamente e che il cluster funzioni nel modo adeguato.

Avvio e arresto manuale dei nodi del cluster

Potrebbe essere necessario arrestare l'intero cluster di failover Kaspersky Security Center Linux o scollegare temporaneamente uno dei nodi del cluster per la manutenzione. In tal caso, seguire le istruzioni contenute in questa sezione. Non tentare di avviare o arrestare i servizi o i processi relativi al cluster di failover utilizzando altri metodi. Questo potrebbe determinare la perdita di dati.

Avvio e arresto dell'intero cluster di failover per la manutenzione

Per avviare o arrestare l'intero cluster di failover:

1. Nel nodo attivo, passare a /opt/kaspersky/ksc64/sbin.
2. Aprire la riga di comando, quindi eseguire uno dei seguenti comandi:
   - Per arrestare il cluster, eseguire: `klfoc -stopcluster --stp klfoc`
   - Per avviare il cluster, eseguire: `klfoc -startcluster --stp klfoc`

Il cluster di failover viene avviato o arrestato, a seconda del comando eseguito.

Manutenzione di uno dei nodi

Per eseguire la manutenzione di uno dei nodi:

1. Nel nodo attivo arrestare il cluster di failover utilizzando il comando `klfoc -stopcluster --stp klfoc`.
2. Nel nodo che si desidera mantenere, passare a /opt/kaspersky/ksc64/sbin.
3. Aprire la riga di comando, quindi scollegare il nodo dal cluster eseguendo il comando `detach_node.sh`.
4. Nel nodo attivo avviare il cluster di failover utilizzando il comando `klfoc -startcluster --stp klfoc`.
5. Eseguire le attività di manutenzione.
6. Nel nodo attivo arrestare il cluster di failover utilizzando il comando `klfoc -stopcluster --stp klfoc`.
7. Nel nodo che è stato mantenuto, passare a /opt/kaspersky/ksc64/sbin.
8. Aprire la riga di comando, quindi collegare il nodo al cluster eseguendo il comando `attach_node.sh`.
9. Nel nodo attivo avviare il cluster di failover utilizzando il comando `klfoc -startcluster --stp klfoc`.

Viene eseguita la manutenzione del nodo, che viene quindi collegato al cluster di failover.

Account per l'utilizzo del DBMS

Per installare Administration Server e utilizzarlo, è necessario un account DBMS interno. Questo account consente di accedere al DBMS e richiede diritti specifici. Un insieme dei diritti richiesti dipende dai seguenti criteri:

- Tipo di DBMS:
  - MySQL o MariaDB
  - PostgreSQL o Postgres Pro
- Metodo di creazione del database di Administration Server:
  - **Automatico**. Durante l'installazione di Administration Server, è possibile creare automaticamente un database di Administration Server (di seguito denominato anche database del server) utilizzando il programma di installazione di Administration Server (il programma di installazione).
  - **Manuale**. È possibile utilizzare un'applicazione di terze parti o uno script per creare un database vuoto. Successivamente, è possibile specificare questo database come database del server durante l'installazione di Administration Server.

Seguire il principio del privilegio minimo quando si concedono diritti e autorizzazioni agli account. Ciò significa che i diritti concessi devono essere sufficienti solo per eseguire le azioni richieste.

Le tabelle seguenti contengono informazioni sui diritti del DBMS che è necessario concedere agli account prima di installare e avviare Administration Server.

MySQL e MariaDB

Se si sceglie MySQL o MariaDB come DBMS, creare un account interno DBMS per accedere al DBMS, quindi concedere a questo account i diritti richiesti. Si noti che il metodo di creazione del database non influisce sull'insieme dei diritti. I diritti richiesti sono elencati di seguito:

- Privilegi dello schema:
  - Database di Administration Server: ALL (ad eseclusione di GRANT OPTION).
  - Schemi di sistema (mysql e sys): SELECT, SHOW VIEW.
  - La procedura memorizzata di sys.table_exists: EXECUTE (se si usa MariaDB 10.5 o versione precedente come DBMS, non è necessario concedere il privilegio EXECUTE).
- Privilegi globali per tutti gli schemi: PROCESS, SUPER.

Per ulteriori informazioni su come configurare i diritti dell'account, consultare Configurazione dell'account DBMS per l'utilizzo di MySQL e MariaDB.

Configurazione dei privilegi per il ripristino dei dati di Administration Server

I diritti concessi all'account DBMS interno sono sufficienti per ripristinare i dati di Administration Server dal backup.

PostgreSQL o Postgres Pro

Se si sceglie PostgreSQL o Postgres Pro come DBMS, è possibile utilizzare l'utente *Postgres* (il ruolo Postgres predefinito) o creare un nuovo ruolo Postgres (di seguito denominato anche ruolo) per accedere al DBMS. A seconda del metodo di creazione del database del server, concedere i diritti richiesti al ruolo come descritto nella tabella seguente. Per ulteriori informazioni su come configurare i diritti del ruolo, consultare Configurazione dell'account DBMS per l'utilizzo di PostgreSQL o Postgres Pro.

Diritti del ruolo Postgres

Creazione automatica del database		Creazione manuale del database
L'utente *Postgres* non richiede diritti aggiuntivi.	Privilegi per un nuovo ruolo: CREATEDB.	Per un nuovo ruolo: • Privilegi sul database di Administration Server: ALL. • Privilegi su tutte le tabelle nello schema pubblico: ALL. • Privilegi su tutte le sequenze nello schema pubblico: ALL.

Configurazione dei privilegi per il ripristino dei dati di Administration Server

Per ripristinare i dati di Administration Server dal backup, il ruolo Postgres utilizzato per accedere al DBMS deve disporre dei diritti di proprietario sul database di Administration Server.

Configurazione dell'account DBMS per l'utilizzo di MySQL e MariaDB

Prerequisiti

Prima di assegnare i diritti all'account DBMS, eseguire le azioni seguenti:

1. Assicurarsi di accedere al sistema con l'account di amministratore locale.
2. Installare un ambiente per l'utilizzo di MySQL o MariaDB.

Configurazione dell'account DBMS per l'installazione di Administration Server

Per configurare l'account DBMS per l'installazione di Administration Server:

1. Eseguire un ambiente per l'utilizzo di MySQL o MariaDB con l'account root creato durante l'installazione del DBMS.
2. Creare un account DBMS interno con una password. Il programma di installazione di Administration Server (di seguito denominato anche programma di installazione) e il servizio Administration Server utilizzeranno questo account DBMS interno per accedere al DBMS.

   Per creare un account DBMS con una password, eseguire il comando seguente:

   ```
   /* Create a user named KSCAdmin and specify the password for KSCAdmin */
   CREATE USER 'KSCAdmin' IDENTIFIED BY '<password>';
   ```

   Se si utilizza MySQL 8.0 o versioni precedenti come DBMS, si noti che per queste versioni l'autenticazione "Caching SHA2 password" non è supportata. Modificare l'autenticazione predefinita da “Caching SHA2 password” a “MySQL native password”:

   - Per creare un account DBMS che utilizzi l'autenticazione "MySQL native password", eseguire il comando seguente:

```
CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
```

- Per modificare l'autenticazione per un account DBMS esistente, eseguire il comando seguente:

  ```
  ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
  ```

3. Concedere i seguenti privilegi all'account DBMS creato:

   - Privilegi dello schema:
     - Database di Administration Server: ALL (ad eseclusione di GRANT OPTION)
     - Schemi di sistema (mysql e sys): SELECT, SHOW VIEW
     - Procedura memorizzata di sys.table_exists: EXECUTE
   - Privilegi globali per tutti gli schemi: PROCESS, SUPER

   Per concedere i privilegi richiesti all'account DBMS creato, eseguire lo script seguente:

   ```
   /* Grant privileges to KSCAdmin */
   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';
   ```

   Se si usa MariaDB 10.5 o versione precedente come DBMS, non è necessario concedere il privilegio EXECUTE. In questo caso, escludere il seguente comando dallo script: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

4. Per visualizzare l'elenco dei privilegi concessi all'account DBMS, eseguire il comando seguente:

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

5. Per creare manualmente un database di Administration Server, eseguire lo script seguente (in questo script, il nome del database di Administration Server è *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   Utilizzare lo stesso nome di database specificato nello script che crea l'account DBMS.

6. Installazione di Administration Server.

Al termine dell'installazione, viene creato il database di Administration Server e Administration Server è pronto per l'uso.

Configurazione dell'account DBMS per l'utilizzo di PostgreSQL e Postgres Pro

Prerequisiti

Prima di assegnare i diritti all'account DBMS, eseguire le azioni seguenti:

1. Assicurarsi di accedere al sistema con l'account di amministratore locale.
2. Installare un ambiente per l'utilizzo di PostgreSQL e Postgres Pro.

Configurazione dell'account DBMS per l'installazione di Administration Server (creazione automatica del database di Administration Server)

Per configurare l'account DBMS per l'installazione di Administration Server:

1. Eseguire un ambiente per l'utilizzo di PostgreSQL e Postgres Pro.
2. Scegliere un ruolo di Postgres per accedere al DBMS. È possibile utilizzare uno dei seguenti ruoli:
   - L'utente *Postgres* (il ruolo predefinito di Postgres).

     Se si usa l'utente *Postgres*, non è necessario concedergli ulteriori diritti.

     Per impostazione predefinita, l'utente *Postgres* non dispone di una password. Tuttavia, è necessaria una password per installare Kaspersky Security Center Linux. Per impostare una password per l'utente *Postgres*, eseguire il seguente script:

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

   - Un nuovo ruolo di Postgres.

     Se si desidera utilizzare un nuovo ruolo di Postgres, creare tale ruolo e concedergli il privilegio CREATEDB. A tale scopo, eseguire il seguente script (in questo script, il ruolo è *KCSAdmin*):

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

     Il ruolo creato verrà utilizzato come proprietario del database di Administration Server (di seguito denominato anche database del server).
3. Installazione di Administration Server.

Al termine dell'installazione, il database del server viene creato automaticamente e Administration Server è pronto per l'uso.

Configurazione dell'account DBMS per l'installazione di Administration Server (creazione manuale del database di Administration Server)

Per configurare l'account DBMS per l'installazione di Administration Server:

1. Eseguire un ambiente per l'utilizzo di Postgres.
2. Creare un nuovo ruolo di Postgres e un database di Administration Server. Quindi, concedere tutti i privilegi al ruolo nel database di Administration Server. A tale scopo, accedere come utente *Postgres* al database *Postgres* ed eseguire il seguente script (in questo script, il ruolo è *KCSAdmin,* il nome del database di Administration Server è *KAV*):

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

Se si verifica l'errore "La nuova codifica (UTF8) non è compatibile con la codifica del database modello", creare un database utilizzando il comando:
`CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;`
anziché:
`CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

3. Concedere i seguenti privilegi al ruolo di Postgres creato:

   - Privilegi su tutte le tabelle nello schema pubblico: ALL
   - Privilegi su tutte le sequenze nello schema pubblico: ALL

   A tale scopo, accedere come utente *Postgres* al database del server ed eseguire il seguente script (in questo script, il ruolo è *KCSAdmin*):

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

4. Installazione di Administration Server.

Al termine dell'installazione, Administration Server utilizzerà il database creato per archiviare i dati di Administration Server. Administration Server è pronto per l'uso.

Certificati per l'utilizzo di Kaspersky Security Center Linux

Questa sezione contiene informazioni sui certificati di Kaspersky Security Center Linux e descrive come emettere e sostituire certificati per Kaspersky Security Center Web Console e come rinnovare un certificato per Administration Server se il Server interagisce con Kaspersky Security Center Web Console.

Informazioni sui certificati di Kaspersky Security Center

Kaspersky Security Center utilizza i seguenti tipi di certificati per consentire un'interazione sicura tra i componenti dell'applicazione:

- Certificato di Administration Server
- Certificato Server Web
- Certificato di Kaspersky Security Center Web Console

Per impostazione predefinita, Kaspersky Security Center utilizza certificati autofirmati (ovvero emessi da Kaspersky Security Center stesso), ma è possibile sostituirli con certificati personalizzati per soddisfare al meglio i requisiti della rete dell'organizzazione e rispettare gli standard di sicurezza. Quando Administration Server verifica che un certificato personalizzato soddisfa tutti i requisiti applicabili, il certificato assume lo stesso ambito funzionale di un certificato autofirmato. L'unica differenza è che un certificato personalizzato non viene riemesso automaticamente alla scadenza. È possibile sostituire i certificati con quelli personalizzati tramite l'utilità klsetsrvcert o la sezione delle proprietà di Administration Server in Kaspersky Security Center Web Console, a seconda del tipo di certificato. Quando si utilizza l'utilità klsetsrvcert, è necessario specificare un tipo di certificato utilizzando uno dei seguenti valori:

- C: certificato comune per le porte 13000 e 13291.
- CR: certificato di riserva comune per le porte 13000 e 13291.

Il periodo di validità massimo di qualsiasi certificato di Administration Server non deve superare i 397 giorni.

Certificati di Administration Server

Un certificato di Administration Server è necessario per i seguenti scopi:

- Autenticazione di Administration Server durante la connessione a Kaspersky Security Center Web Console
- Interazione sicura tra Administration Server e Network Agent nei dispositivi gestiti
- Autenticazione quando gli Administration Server primari sono connessi agli Administration Server secondari

Il certificato di Administration Server viene creato automaticamente durante l'installazione del componente Administration Server e viene archiviato nella cartella /var/opt/kaspersky/klnagent_srv/1093/cert/. Specificare il certificato di Administration Server quando si crea un file di risposta per installare Kaspersky Security Center Web Console. Questo certificato è denominato comune ("C").

Il certificato di Administration Server è valido per 397 giorni. Kaspersky Security Center genera automaticamente un certificato ("CR") di riserva comune 90 giorni prima della scadenza del certificato comune. Il certificato di riserva comune viene successivamente utilizzato per la sostituzione immediata del certificato di Administration Server. Quando il certificato comune sta per scadere, il certificato di riserva comune viene utilizzato per gestire la connessione con le istanze di Network Agent installate nei dispositivi gestiti. A tale scopo, il certificato di riserva comune diventa automaticamente il nuovo certificato comune 24 ore prima della scadenza del certificato comune precedente.

Il periodo di validità massimo di qualsiasi certificato di Administration Server non deve superare i 397 giorni.

Se necessario, è possibile assegnare un certificato personalizzato per Administration Server. Questo può ad esempio essere necessario per una migliore integrazione con l'infrastruttura PKI esistente dell'azienda o per la configurazione personalizzata dei campi dei certificati. Quando si sostituisce il certificato, tutti i Network Agent che sono stati precedentemente connessi ad Administration Server tramite SSL perderanno la connessione e restituiranno un errore di autenticazione di Administration Server. Per eliminare l'errore, sarà necessario ripristinare la connessione dopo la sostituzione del certificato.

In caso di smarrimento del certificato di Administration Server, è necessario reinstallare il componente Administration Server e ripristinare i dati per recuperarlo.

È inoltre possibile eseguire il backup del certificato di Administration Server separatamente dalle altre impostazioni di Administration Server per spostare Administration Server da un dispositivo all'altro senza perdite di dati.

Certificati mobili

Per l'autenticazione di Administration Server nei dispositivi mobili è richiesto un certificato mobile ("M"). Il certificato mobile viene specificato nelle proprietà di Administration Server.

Esiste inoltre un certificato di riserva mobile ("MR"): viene utilizzato per la sostituzione immediata del certificato mobile. Kaspersky Security Center genera automaticamente questo certificato 60 giorni prima della scadenza del certificato comune. Quando il certificato mobile sta per scadere, il certificato di riserva mobile viene utilizzato per gestire la connessione con le istanze di Network Agent installate nei dispositivi mobili gestiti. A tale scopo, il certificato di riserva mobile diventa automaticamente il nuovo certificato mobile 24 ore prima della scadenza del certificato mobile precedente.

Se lo scenario di connessione richiede l'utilizzo di un certificato client nei dispositivi mobili (connessione che implica l'autenticazione SSL bidirezionale), è possibile generare tali certificati tramite l'autorità di certificazione per i certificati utente generati automaticamente ("MCA"). Inoltre, nelle proprietà di Administration Server, è possibile specificare certificati client personalizzati emessi da un'altra autorità di certificazione, mentre l'integrazione con l'infrastruttura a chiave pubblica (PKI) del dominio dell'organizzazione consente di emettere certificati client tramite l'autorità di certificazione del dominio.

Certificato Server Web

Il server Web, un componente di Kaspersky Security Center Administration Server, utilizza un tipo speciale di certificato. Questo certificato è necessario per pubblicare i pacchetti di installazione di Network Agent che vengono successivamente scaricati nei dispositivi gestiti. A tale scopo, Server Web può utilizzare diversi certificati.

Server Web utilizza uno dei seguenti certificati, in ordine di priorità:

1. Certificato Server Web personalizzato specificato manualmente tramite Kaspersky Security Center Web Console

2. Certificato di Administration Server comune ("C")

Certificato di Kaspersky Security Center Web Console

Il server di Kaspersky Security Center Web Console (di seguito denominato Web Console) dispone di un proprio certificato. Quando si apre un sito Web, un browser verifica se la connessione è attendibile. Il certificato di Web Console consente di autenticare Web Console e viene utilizzato per criptare il traffico tra un browser e Web Console.

Quando si apre Web Console, il browser potrebbe informare che la connessione a Web Console non è privata e il certificato Web Console non è valido. Questo avviso viene visualizzato perché il certificato di Web Console è autofirmato e generato automaticamente da Kaspersky Security Center. Per rimuovere questo avviso è possibile eseguire una delle seguenti operazioni:

- Sostituire il certificato di Web Console con uno personalizzato (opzione consigliata). Creare un certificato attendibile nella propria infrastruttura e che soddisfi i requisiti per i certificati personalizzati.

- Aggiungere il certificato di Web Console all'elenco dei certificati del browser attendibili. È consigliabile utilizzare questa opzione solo se non è possibile creare un certificato personalizzato.

Requisiti per i certificati personalizzati utilizzati in Kaspersky Security Center Linux

La seguente tabella visualizza i requisiti per i certificati personalizzati specificati per i diversi componenti di Kaspersky Security Center Linux.

Requisiti per i certificati di Kaspersky Security Center Linux

Tipo di certificato	Requisiti	Commenti
Certificato comune, certificato di riserva comune ("C", "CR")	Lunghezza minima della chiave: 2048. Vincoli di base: • Vincolo lunghezza percorso: nessuno Utilizzo chiave: • Firma digitale • Firma del certificato • Cifratura chiave • Firma CRL Utilizzo chiavi esteso (opzionale): autenticazione del server, autenticazione del client.	Il parametro Utilizzo chiavi esteso è facoltativo. Il valore Vincolo lunghezza percorso può essere un valore intero diverso da "Nessuno", ma non inferiore a 1.
Certificato Server Web	Utilizzo chiavi esteso: autenticazione del server. Il contenitore PKCS #12 / PEM da cui viene specificato il certificato include l'intera catena di chiavi pubbliche. È presente il Nome alternativo soggetto del certificato; quindi il valore del campo `subjectAltName` è valido. Il certificato soddisfa i requisiti effettivi dei browser Web imposti ai certificati del server, nonché gli attuali requisiti di base del CA/Browser Forum.	—
Certificato di Kaspersky Security Center Web Console	Il contenitore PEM da cui viene specificato il certificato include l'intera catena di chiavi pubbliche. È presente il Nome alternativo soggetto del certificato; quindi il valore del campo `subjectAltName` è valido. Il certificato soddisfa i requisiti effettivi dei browser Web per i certificati del server, nonché gli attuali requisiti di base del CA/Browser Forum.	I certificati criptati non sono supportati da Kaspersky Security Center Web Console.

Riemissione del certificato per Kaspersky Security Center Web Console

La maggior parte dei browser impone un limite relativo al periodo di validità di un certificato. Per rientrare in questo limite, il periodo di validità del certificato di Kaspersky Security Center Web Console è limitato a 397 giorni. È possibile sostituire un certificato esistente ricevuto da un'autorità di certificazione (CA) emettendo manualmente un nuovo certificato autofirmato. In alternativa, è possibile riemettere il certificato scaduto di Kaspersky Security Center Web Console.

La riemissione automatica del certificato per Kaspersky Security Center Web Console non è supportata È necessario riemettere manualmente il certificato scaduto.

Quando si apre Kaspersky Security Center Web Console, il browser può segnalare che la connessione a Kaspersky Security Center Web Console non è privata e il certificato di Kaspersky Security Center Web Console non è valido. Questo avviso viene visualizzato perché il certificato di Web Console è autofirmato e generato automaticamente da Kaspersky Security Center Linux. Per rimuovere o impedire questo avviso, è possibile eseguire una delle seguenti operazioni:

- Specificare un certificato personalizzato quando lo si emette nuovamente (opzione consigliata). Creare un certificato attendibile nella propria infrastruttura e che soddisfi i requisiti per i certificati personalizzati.
- Aggiungere il certificato di Kaspersky Security Center Web Console all'elenco dei certificati del browser attendibili dopo la riemissione del certificato. È consigliabile utilizzare questa opzione solo se non è possibile creare un certificato personalizzato.

Per riemettere il certificato scaduto di Kaspersky Security Center Web Console:

Reinstallare Kaspersky Security Center Web Console eseguendo una delle seguenti operazioni:

- Se si desidera utilizzare lo stesso file di installazione di Kaspersky Security Center Web Console, rimuovere Kaspersky Security Center Web Console, quindi installare la stessa versione di Kaspersky Security Center Web Console.
- Se si desidera utilizzare un file di installazione di una versione aggiornata, eseguire il comando di upgrade.

Il certificato di Kaspersky Security Center Web Console viene riemesso per un altro periodo di validità di 397 giorni.

Sostituzione del certificato per Kaspersky Security Center Web Console

Per impostazione predefinita, quando si installa Kaspersky Security Center Web Console Server (anche noto come Kaspersky Security Center Web Console), viene generato automaticamente un certificato del browser per l'applicazione. È possibile sostituire il certificato generato automaticamente con uno personalizzato.

Per sostituire il certificato per Kaspersky Security Center Web Console con uno personalizzato:

1. Creare un nuovo file di risposta richiesto per l'installazione di Kaspersky Security Center Web Console.
2. In questo file specificare i percorsi del file di certificato personalizzato e del file chiave utilizzando il parametro `certPath` e il parametro `keyPath`.
3. Reinstallare Kaspersky Security Center Web Console specificando il nuovo file di risposta. Eseguire una delle seguenti operazioni:
   - Se si desidera utilizzare lo stesso file di installazione di Kaspersky Security Center Web Console, rimuovere Kaspersky Security Center Web Console, quindi installare la stessa versione di Kaspersky Security Center Web Console.
   - Se si desidera utilizzare un file di installazione di una versione aggiornata, eseguire il comando di upgrade.

Kaspersky Security Center Web Console funziona con il certificato specificato.

Conversione di un certificato PFX nel formato PEM

Per utilizzare un certificato PFX in Kaspersky Security Center Web Console, è prima necessario convertirlo nel formato PEM utilizzando un'utilità multipiattaforma basata su OpenSSL.

Per convertire un certificato PFX nel formato PEM nel sistema operativo Linux:

1. In un'utilità multipiattaforma basata su OpenSSL, eseguire i seguenti comandi:

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <filename.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Assicurarsi che il file del certificato e la chiave privata siano generati nella stessa directory in cui è archiviato il file .pfx.

3. Kaspersky Security Center Web Console non supporta i certificati protetti da passphrase. Pertanto, eseguire il comando seguente in un'utilità multipiattaforma basata su OpenSSL per rimuovere una passphrase dal file .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Non utilizzare lo stesso nome per i file .pem di input e output.

   Di conseguenza, il nuovo file .pem non risulta criptato. Non è necessario inserire una passphrase per utilizzarlo.

I file .crt e .pem sono pronti per l'uso e possono essere specificati nel programma di installazione di Kaspersky Security Center Web Console.

Scenario: Specificazione del certificato di Administration Server personalizzato

È possibile assegnare il certificato di Administration Server personalizzato, ad esempio per una migliore integrazione con l'infrastruttura a chiave pubblica (PKI) esistente dell'azienda o per la configurazione personalizzata dei campi del certificato. È consigliabile sostituire il certificato subito dopo l'installazione di Administration Server e prima del completamento dell'Avvio rapido guidato.

Il periodo di validità massimo di qualsiasi certificato di Administration Server non deve superare i 397 giorni.

Prerequisiti

Il nuovo certificato deve essere creato nel formato PKCS#12 (ad esempio tramite l'infrastruttura PKI dell'organizzazione) e deve essere rilasciato da un'autorità di certificazione (CA) attendibile. Inoltre, il nuovo certificato deve includere l'intera catena di attendibilità e una chiave privata, che deve essere archiviata nel file con estensione pfx o p12. Per il nuovo certificato devono essere soddisfatti i requisiti elencati di seguito.

Tipo di certificato: certificato comune, certificato di riserva comune ("C", "CR")

Requisiti:

- Lunghezza minima della chiave: 2048
- Vincoli di base:
  - CA: true
  - Vincolo lunghezza percorso: nessuno

    Il valore Vincolo lunghezza percorso può essere un valore intero diverso da "Nessuno" ma non inferiore a 1.
- Utilizzo chiave:
  - Firma digitale
  - Firma del certificato
  - Cifratura chiave

- Firma CRL

- EKU (Extended Key Usage): autenticazione del server e autenticazione del client. Il parametro EKU è facoltativo, ma se il certificato lo contiene, i dati di autenticazione del server e del client devono essere specificati nell'EKU.

I certificati rilasciati da un'autorità di certificazione pubblica non dispongono dell'autorizzazione di firma del certificato. Per utilizzare tali certificati, assicurarsi di aver installato Network Agent versione 13 o successiva nei punti di distribuzione o nei gateway di connessione della rete. In caso contrario, non sarà possibile utilizzare i certificati senza l'autorizzazione di firma.

Passaggi

Sono necessari alcuni passaggi per specificare il certificato di Administration Server:

1. **Sostituzione del certificato di Administration Server**

   A tale scopo, utilizzare la riga di comando utilità klsetsrvcert.

2. **Specificazione di un nuovo certificato e ripristino della connessione dei Network Agent ad Administration Server**

   Quando il certificato viene sostituito, tutti i Network Agent precedentemente connessi ad Administration Server tramite SSL perdono la connessione e restituiscono un errore di autenticazione di Administration Server. Per specificare il nuovo certificato e ripristinare la connessione, utilizzare l'utilità klmover della riga di comando.

Risultati

Al termine dello scenario, il certificato di Administration Server viene sostituito e il server viene autenticato dai Network Agent nei dispositivi gestiti.

Sostituzione del certificato di Administration Server con l'utilità klsetsrvcert

Per sostituire il certificato di Administration Server:

Dalla riga di comando eseguire la seguente utilità:

```
klsetsrvcert [-t <type> {-i <inputfile> [-p <password>] [-o <chkopt>] | -g <dnsname>}][-f <time>][-r <calistfile>]
[-l <logfile>]
```

Non è necessario scaricare l'utilità klsetsrvcert. È inclusa nel kit di distribuzione di Kaspersky Security Center Linux. Non è compatibile con le versioni precedenti di Kaspersky Security Center Linux.

La descrizione dei parametri dell'utilità klsetsrvcert è contenuta nella seguente tabella.

Valori dei parametri dell'utilità klsetsrvcert

Parametro	Valore
`-t <type>`	Tipo del certificato da sostituire. Possibili valori del parametro `<type>`: • `C` – Sostituire il certificato comune per le porte 13000 e 13291.

	• `CR` – Sostituire il certificato di riserva comune per le porte 13000 e 13291.
`-f <time>`	Pianificazione per la modifica del certificato, utilizzando il formato "GG-MM-AAAA hh:mm" (per le porte 13000 e 13291). Utilizzare questo parametro se si desidera sostituire il certificato comune con il certificato di riserva comune prima della scadenza del certificato comune. Specificare l'ora in cui i dispositivi gestiti devono sincronizzarsi con Administration Server in un nuovo certificato.
`-i <inputfile>`	Contenitore con il certificato e una chiave privata nel formato PKCS#12 (file con estensione p12 o pfx).
`-p <password>`	Password utilizzata per la protezione del contenitore p12. Il certificato e una chiave privata vengono archiviati nel contenitore, pertanto è necessaria la password per decriptare il file con il contenitore.
`-o <chkopt>`	Parametri di convalida del certificato (separati da punto e virgola). Per utilizzare un certificato personalizzato senza l'autorizzazione di firma, specificare `-o NoCA` nell'utilità klsetsrvcert. Questo è utile per i certificati rilasciati da un'autorità di certificazione pubblica. Per modificare la lunghezza della chiave di criptaggio per i tipi di certificato C o CR, specificare `-o RsaKeyLen:< lunghezza della chiave >` nell'utilità klsetsrvcert, dove il parametro `< lunghezza della chiave >` è il valore della lunghezza della chiave richiesto. In caso contrario, viene utilizzata la lunghezza della chiave del certificato corrente.
`-g <dnsname>`	Verrà creato un nuovo certificato per il nome DNS specificato.
`-r <calistfile>`	Elenco delle autorità di certificazione radice attendibili, formato PEM.
`-l <logfile>`	File di output dei risultati. Per impostazione predefinita, l'output viene reindirizzato nel flusso di output standard.

Per specificare il certificato personalizzato di Administration Server, utilizzare ad esempio il seguente comando:

```
klsetsrvcert -t C -i <inputfile> -p <password> -o NoCA
```

Dopo la sostituzione del certificato, tutti i Network Agent connessi ad Administration Server tramite SSL perdono la connessione. Per ripristinarla, utilizzare l'utilità klmover della riga di comando.

Per evitare di perdere le connessioni di Network Agent, utilizzare i seguenti comandi:

1. Per installare il nuovo certificato,

   ```
   klsetsrvcert -t CR -i <inputfile> -p <password> -o NoCA
   ```

2. Per specificare la data in cui verrà applicato il nuovo certificato,

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

dove "`DD-MM-YYYY hh:mm`" è la data di 3-4 settimane successive alla data attuale. Lo slittamento temporale per la modifica del certificato in uno nuovo consentirà la distribuzione del nuovo certificato a tutti i Network Agent.

Connessione dei Network Agent ad Administration Server con l'utilità klmover

È possibile utilizzare l'utilità klmover per ripristinare la connessione da dispositivi non controllati ad Administration Server, ad esempio dopo un errore di Administration Server, se non è possibile eseguire il ripristino da un backup.

Per ripristinare la connessione eseguire l'utilità klmover dalla riga di comando:

- Per Linux:
  - Per i sistemi a 32 bit: `/opt/kaspersky/klnagent/bin/klmover [-address <indirizzo server>] [-pn <numero porta>] [-ps <numero porta SSL>] [-nossl] [-cert <percorso del file di certificato>]`
  - Per i sistemi a 64 bit: `/opt/kaspersky/klnagent64/bin/klmover [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-nossl] [-cert <path to certificate file>]`
- Per Windows:
  - Per i sistemi a 32 bit: `<percorso>\klmover.exe [-address <indirizzo server>] [-pn <numero porta>] [-ps <numero porta SSL>] [-nossl] [-cert <percorso del file di certificato>]`
  - Per i sistemi a 64 bit: `<percorso>\klmover.exe [-address <indirizzo server>] [-pn <numero porta>] [-ps <numero porta SSL>] [-nossl] [-cert <percorso del file di certificato>]`

dove `<percorso>` è il percorso di installazione predefinito per Network Agent oppure il percorso di installazione specificato dall'utente nelle impostazioni del pacchetto di installazione di Network Agent.

Per impedire agli intrusi di spostare i dispositivi fuori dal controllo di Administration Server, si consiglia di abilitare la protezione tramite password per l'esecuzione dell'utilità klmover. Per abilitare la protezione con password, selezionare l'opzione **Usa password di disinstallazione** nelle impostazioni dei criteri di Network Agent.

Se si perde o si dimentica la password di Network Agent protetto da password installato nel dispositivo che non è più sotto la gestione di Kaspersky Security Center Linux, non è possibile rimuovere Network Agent utilizzando l'utilità klmover o il prompt dei comandi. In questo caso, è necessario reinstallare il sistema operativo nel dispositivo in cui è installato Network Agent protetto da password.

L'utilità klmover richiede i diritti di amministratore locale.

L'abilitazione dell'opzione **Usa password di disinstallazione** nei dispositivi Windows consente anche di abilitare la protezione tramite password per lo strumento Cleaner (cleaner.exe).

Non è possibile utilizzare l'utilità klmover per i dispositivi client connessi ad Administration Server tramite gateway di connessione. Per tali dispositivi è necessario riconfigurare Network Agent o reinstallarlo e specificare il gateway di connessione.

La descrizione dei parametri dell'utilità klmover è contenuta nella seguente tabella.

Valori dei parametri dell'utilità klmover

Parametro	Valore
`-address <indirizzo server>`	Indirizzo di Administration Server per la connessione. È possibile specificare un indirizzo IP o il nome DNS.
`-pn <numero di porta>`	Numero della porta tramite la quale viene stabilita la connessione non criptata ad Administration Server. Il numero di porta predefinito è 14000.
`-ps <numero di porta SSL>`	Numero della porta SSL tramite la quale viene stabilita la connessione criptata ad Administration Server utilizzando il protocollo SSL. Il numero di porta predefinito è 13000.

`-nossl`	Utilizza la connessione non criptata ad Administration Server. Se la chiave non è in uso, Network Agent è connesso ad Administration Server tramite il protocollo SSL criptato.
`-cert <percorso del file di certificato>`	Utilizzare il file di certificato specificato per l'autenticazione dell'accesso ad Administration Server.

Definizione di una cartella condivisa

Dopo l'installazione dell'Administration Server, è possibile specificare il percorso della cartella condivisa nelle proprietà dell'Administration Server. Per impostazione predefinita, la cartella condivisa viene creata nel dispositivo con l'Administration Server. Tuttavia, in alcuni casi (ad esempio, carico elevato o esigenza di accesso da una rete isolata) è consigliabile posizionare la cartella condivisa in una risorsa file dedicata.

La cartella condivisa viene utilizzata occasionalmente durante la distribuzione di Network Agent.

La distinzione tra maiuscole e minuscole per la cartella condivisa deve essere disabilitata.

Accesso a Kaspersky Security Center Web Console e disconnessione

È possibile accedere a Kaspersky Security Center Web Console dopo aver installato Administration Server e Web Console Server. È necessario conoscere l'indirizzo Web di Administration Server e il numero di porta specificato durante l'installazione (per impostazione predefinita, la porta è 8080). JavaScript deve essere abilitato nel browser.

Per accedere a Kaspersky Security Center Web Console:

1. Nel browser visitare <indirizzo Web di Administration Server>:<numero di porta>.

   Viene visualizzata la pagina di accesso.

2. Se sono stati aggiunti più server attendibili, nell'elenco Administration Server selezionare l'Administration Server a cui si desidera connettersi.

   Se è stato aggiunto un solo Administration Server, l'elenco degli Administration Server è bloccato.

3. Eseguire una delle seguenti operazioni:

   - Per accedere ad Administration Server con un account utente di dominio, immettere il nome utente e la password dell'utente di dominio.

     È possibile immettere il nome utente dell'utente del dominio in uno dei seguenti formati:

     - `Username@dns.domain`
     - `NTDOMAIN\Username`

     Prima di accedere con un account utente di dominio, eseguire il polling del controller di dominio per ottenere l'elenco degli utenti di dominio.

   - Per accedere ad Administration Server specificando il nome utente e la password dell'amministratore, immettere il nome utente e la password dell'utente interno.

- Se nel server vengono creati uno o più Administration Server virtuali e si desidera accedere a un server virtuale:

  a. Fare clic su **Mostra opzioni server virtuale**.

  b. Digitare il nome dell'Administration Server virtuale specificato durante la creazione del server virtuale.

  c. Immettere il nome utente e la password dell'amministratore che dispone dei diritti sull'Administration Server virtuale.

4. Fare clic sul pulsante **Accedi**.

Dopo l'accesso, viene visualizzato il dashboard, con la lingua e il tema utilizzati l'ultima volta. È possibile spostarsi in Kaspersky Security Center Web Console e utilizzarlo per lavorare con Kaspersky Security Center Linux.

Disconnessione

Per eseguire la disconnessione da Kaspersky Security Center Web Console:

Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Esci**.

Kaspersky Security Center Web Console verrà chiuso e sarà visualizzata la pagina di accesso.

Modifica della lingua dell'interfaccia di Kaspersky Security Center Web Console

È possibile selezionare la lingua dell'interfaccia di Kaspersky Security Center Web Console.

Per modificare la lingua dell'interfaccia:

1. Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Lingua**.
2. Selezionare una delle lingue di localizzazione supportate.

Configurazione del server MySQL x64 per l'utilizzo con Kaspersky Security Center Linux

Se si utilizza il server MySQL per Kaspersky Security Center, abilitare il supporto per InnoDB e l'archiviazione MEMORY, nonché per le codifiche UTF-8 e UCS-2.

Impostazioni consigliate per il file my.cnf

Per maggiori dettagli sulla configurazione del DBMS, fare riferimento anche alla procedura di configurazione dell'account. Per informazioni sull'installazione del DBMS, fare riferimento alla procedura di installazione del DBMS.

Per configurare il file my.cnf:

1. Aprire il file my.cnf in un editor di testo.

2. Aggiungere le seguenti righe nella sezione `[mysqld]` del file my.cnf:

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size= il valore reale non deve essere inferiore all'80% delle
dimensioni previste del database KAV
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (nella maggior parte dei casi il server utilizza
piccole transazioni)
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
```

Si noti che la memoria specificata nel valore `innodb_buffer_pool_size` viene allocato all'avvio del server. Se la dimensione del database è inferiore alla dimensione del buffer specificata, viene allocata solo la memoria richiesta. La dimensione effettiva della memoria allocata è di circa il 10% maggiore rispetto alla dimensione del buffer specificata. Per ulteriori dettagli, consultare la documentazione di MySQL.

È consigliabile utilizzare il valore del parametro `innodb_flush_log_at_trx_commit = 0`, perché i valori "1" o "2" influiscono negativamente sulla velocità di esecuzione di MySQL. Assicurarsi che il parametro `innodb_file_per_table` sia impostato su `1`.

Avvio rapido guidato

Kaspersky Security Center Linux consente di regolare una selezione minima di impostazioni necessarie per creare un sistema centralizzato di gestione per la protezione della rete dalle minacce per la sicurezza. Questa configurazione viene eseguita tramite l'Avvio rapido guidato. Quando la procedura guidata è in esecuzione, è possibile apportare le seguenti modifiche all'applicazione:

- Aggiungere file chiave o immettere codici di attivazione che è possibile distribuire automaticamente ai dispositivi nei gruppi di amministrazione.
- Impostare l'invio tramite e-mail delle notifiche degli eventi che si verificano durante il funzionamento di Administration Server e delle applicazioni gestite.
- Creare un criterio di protezione per workstation e server, nonché attività di scansione malware, attività di download degli aggiornamenti e attività di backup dei dati, per il livello superiore della gerarchia dei dispositivi gestiti.

  L'Avvio rapido guidato crea criteri soltanto per le applicazioni per cui non sono presenti criteri nella cartella **Dispositivi gestiti**. L'Avvio rapido guidato non crea attività se sono già state create attività con lo stesso nome per il livello superiore della gerarchia dei dispositivi gestiti.

L'applicazione richiede automaticamente di eseguire l'Avvio rapido guidato dopo l'installazione di Administration Server, al momento della prima connessione. È anche possibile avviare manualmente l'avvio rapido guidato in qualsiasi momento.

Per avviare manualmente l'avvio rapido guidato:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome di Administration Server.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Generale**.

3. Fare clic su **Esegui l'Avvio rapido guidato**.

Verrà offerta la possibilità di eseguire la configurazione iniziale di Administration Server. Seguire le istruzioni della procedura guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

Passaggio 1. Definizione delle impostazioni della connessione Internet

Specificare le impostazioni di accesso a Internet per Administration Server. È necessario configurare l'accesso a Internet per utilizzare Kaspersky Security Network e per scaricare gli aggiornamenti dei database anti-virus per Kaspersky Security Center Linux e le applicazioni Kaspersky gestite.

Se si desidera utilizzare un server proxy durante la connessione a Internet, abilitare l'opzione **Usa server proxy**. Se questa opzione è abilitata, i campi sono disponibili per l'immissione delle impostazioni. Specificare le seguenti impostazioni per la connessione a un server proxy:

- **Indirizzo**

  Indirizzo del server proxy utilizzato per la connessione di Kaspersky Security Center Linux a Internet.

- **Numero di porta**

  Numero della porta utilizzata per stabilire la connessione al proxy di Kaspersky Security Center Linux.

- **Ignora il server proxy per gli indirizzi locali**

  Non verrà utilizzato alcun server proxy per la connessione ai dispositivi dalla rete locale.

- **Autenticazione server proxy**

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

  Questo campo di immissione è disponibile se la casella di controllo **Usa server proxy** è selezionata.

- **Nome utente**

  Account utente con il quale è stata stabilita la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

- **Password**

Password impostata dall'utente di cui è stato utilizzato l'account per stabilire la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

Per visualizzare la password immessa, tenere premuto il pulsante **Mostra** per il tempo necessario.

È possibile configurare l'accesso a Internet in un secondo momento, separatamente dall'Avvio rapido guidato.

Passaggio 2. Download degli aggiornamenti necessari

Gli aggiornamenti richiesti vengono scaricati automaticamente dai server Kaspersky.

Passaggio 3. Selezione delle risorse da proteggere

Selezionare le aree di protezione e i sistemi operativi in uso nella rete. Quando si selezionano queste opzioni, si specificano i filtri per i plug-in di gestione delle applicazioni e i pacchetti di distribuzione nei server Kaspersky che è possibile scaricare per installarli nei dispositivi client nella rete.

Selezionare le opzioni:

- Aree

  È possibile selezionare i seguenti ambiti di protezione:
  - **Workstation**
  - **File server e archiviazione**
  - **Virtualizzazione**
  - **Sistemi incorporati**
  - **Reti industriali**
  - **Endpoint industriali**

- Sistemi operativi

  È possibile selezionare le seguenti piattaforme:
  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Altro

  Per ulteriori informazioni sui sistemi operativi supportati, vedere Requisiti hardware e software per Kaspersky Security Center Web Console.

È possibile selezionare i pacchetti dell'applicazione Kaspersky nell'elenco dei pacchetti disponibili in un secondo momento, separatamente dall'Avvio rapido guidato. Per semplificare la ricerca dei pacchetti richiesti, è possibile filtrare l'elenco dei pacchetti disponibili in base a vari criteri.

Passaggio 4. Selezione del criptaggio nelle soluzioni

La finestra **Criptaggio nelle soluzioni** viene visualizzata solo se è stato selezionato **Workstation** come ambito della protezione.

Kaspersky Endpoint Security for Windows include strumenti di criptaggio per le informazioni archiviate nei dispositivi client basati su Windows. In tali strumenti di criptaggio, è implementato AES (Advanced Encryption Standard), con una lunghezza della chiave di 256 o 56 bit.

Il download e l'utilizzo del pacchetto di distribuzione con una lunghezza della chiave di 256 bit devono essere eseguiti in conformità con le leggi e le normative applicabili. Per scaricare un pacchetto di distribuzione di Kaspersky Endpoint Security for Windows valido per le esigenze aziendali, consultare le normative del paese in cui si trovano i dispositivi client dell'organizzazione.

Nella finestra **Criptaggio nelle soluzioni** selezionare uno dei seguenti tipi di criptaggio:

- Crittografia Lite. Questo tipo di criptaggio utilizza una lunghezza della chiave di 56 bit.
- Crittografia avanzata. Questo tipo di criptaggio utilizza una lunghezza della chiave di 256 bit.

È possibile selezionare il pacchetto di distribuzione per Kaspersky Endpoint Security for Windows con il tipo di criptaggio richiesto in un secondo momento, separatamente dall'Avvio rapido guidato.

Passaggio 5. Configurazione dell'installazione dei plug-in per le applicazioni gestite

Selezionare i plug-in per le applicazioni gestite da installare. Viene visualizzato un elenco dei plug-in che si trovano nei server Kaspersky. L'elenco viene filtrato in base alle opzioni selezionate nel passaggio precedente della procedura guidata. Per impostazione predefinita, un elenco completo include i plug-in di tutte le lingue. Per visualizzare solo i plug-in di una lingua specifica, utilizzare il filtro.

L'elenco dei plug-in include le seguenti colonne:

- Area da proteggere

  Le aree selezionate da proteggere sono visualizzate in questa colonna.

- Tipo

  I tipi di plug-in vengono visualizzati in questa colonna.

- Nome

  I plug-in sono selezionati in base alle aree di protezione e alle piattaforme, selezionati nel passaggio precedente.

- **Versione**

  L'elenco include i plug-in di tutte le versioni che si trovano nei server Kaspersky. Per impostazione predefinita, sono selezionati i plug-in delle versioni più recenti.

- **Versione più recente**

  Questa colonna indica se una versione del plug-in è l'ultima. Se viene visualizzato il valore **true**, il plug-in corrispondente è della versione più recente. Se viene visualizzato un valore **false**, il plug-in corrispondente ha una versione successiva.

- **Sistema operativo**

  Questa colonna mostra i sistemi operativi dei plug-in.

- **Lingua**

  Per impostazione predefinita, la lingua di localizzazione di un plug-in è determinata dalla lingua di Kaspersky Security Center Linux selezionata al momento dell'installazione. È possibile specificare altre lingue nell'elenco a discesa **Mostra lingua di localizzazione di Administration Console oppure**.

Dopo aver selezionato i plug-in, fare clic su **Avanti** per avviare l'installazione.

È possibile installare i plug-in di gestione per le applicazioni Kaspersky manualmente, separatamente dall'Avvio rapido guidato.

L'Avvio rapido guidato installa automaticamente i plug-in selezionati. Per installare alcuni plug-in è necessario accettare le condizioni del Contratto di licenza con l'utente finale. Leggere il testo del Contratto di licenza con l'utente finale visualizzato, selezionare la casella di controllo **Accetto di utilizzare Kaspersky Security Network** e fare clic sul pulsante **Installa**. Se non si accettano le condizioni del Contratto di licenza con l'utente finale, il plug-in non viene installato.

Quando tutti i plug-in selezionati sono installati, l'Avvio rapido guidato porta automaticamente al passaggio successivo.

Passaggio 6. Download dei pacchetti di distribuzione e creazione dei pacchetti di installazione

Selezionare i pacchetti di distribuzione da scaricare.

Le distribuzioni delle applicazioni gestite potrebbero richiedere l'installazione di una versione minima specifica di Kaspersky Security Center Linux.

Dopo aver selezionato un tipo di criptaggio per Kaspersky Endpoint Security for Windows, viene visualizzato un elenco dei pacchetti di distribuzione di entrambi i tipi di criptaggio. Nell'elenco viene selezionato un pacchetto di distribuzione con il tipo di criptaggio selezionato. È possibile selezionare i pacchetti di distribuzione di qualsiasi tipo di criptaggio. La lingua del pacchetto di distribuzione corrisponde alla lingua di Kaspersky Security Center Linux. Se non esiste un pacchetto di distribuzione dell'applicazione per la lingua di Kaspersky Security Center Linux, viene selezionato il pacchetto di distribuzione in lingua inglese.

Per terminare il download di alcuni pacchetti di distribuzione è necessario accettare il Contratto di licenza con l'utente finale. Quando si fa clic sul pulsante **Accetta**, viene visualizzato il testo del Contratto di licenza con l'utente finale. Per procedere al passaggio successivo della procedura guidata, è necessario accettare i termini e le condizioni del Contratto di licenza con l'utente finale e i termini e le condizioni dell'Informativa sulla privacy di Kaspersky. Se non si accettano i termini e le condizioni, il download del pacchetto viene annullato.

Dopo aver accettato i termini e le condizioni del Contratto di licenza con l'utente finale e i termini e le condizioni dell'Informativa sulla privacy di Kaspersky, il download dei pacchetti di distribuzione prosegue. Successivamente è possibile utilizzare i pacchetti di installazione per distribuire le applicazioni Kaspersky nei dispositivi client.

Passaggio 7. Configurazione di Kaspersky Security Network

Specificare le impostazioni per la trasmissione delle informazioni sulle operazioni di Kaspersky Security Center Linux alla Knowledge Base di Kaspersky Security Network.

Selezionare una delle seguenti opzioni:

- **Accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center Linux e le applicazioni gestite installate nei dispositivi client trasferiranno automaticamente i dettagli sull'esecuzione a Kaspersky Security Network. La partecipazione a Kaspersky Security Network garantisce aggiornamenti più rapidi dei database contenenti le informazioni sui virus e sulle altre minacce, assicurando una risposta più rapida alle minacce per la sicurezza emergenti.

- **Non accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center Linux e le applicazioni gestite non forniranno informazioni a Kaspersky Security Network.

  Se si seleziona questa opzione, l'utilizzo di Kaspersky Security Network sarà disabilitato.

È possibile configurare l'accesso a Kaspersky Security Network (KSN) successivamente, separatamente dall'Avvio rapido guidato.

Passaggio 8. Selezione del metodo di attivazione dell'applicazione

Selezionare una delle seguenti opzioni di attivazione di Kaspersky Security Center Linux:

- **Immettendo il codice di attivazione**

Codice di attivazione è una sequenza univoca di 20 caratteri alfanumerici. Il codice di attivazione viene inserito per aggiungere una chiave che consente di attivare Kaspersky Security Center Linux. Si riceve il codice di attivazione tramite l'indirizzo e-mail specificato dopo l'acquisto di Kaspersky Security Center.

Per attivare l'applicazione utilizzando un codice di attivazione, è necessario l'accesso a Internet per stabilire la connessione con i server di attivazione Kaspersky.

Se è stata selezionata questa opzione di attivazione, è possibile abilitare l'opzione **Distribuisci automaticamente la chiave di licenza ai dispositivi gestiti**.

Se questa opzione è abilitata, la chiave di licenza verrà distribuita automaticamente ai dispositivi gestiti.

Se questa opzione è disabilitata, è possibile distribuire la chiave di licenza ai dispositivi gestiti in un secondo momento, nella sezione **Operazioni** → **Licensing** → **Licenze di Kaspersky** del menu principale.

- Specificando un file chiave

File chiave: si tratta di un file con estensione key fornito all'utente da Kaspersky. Un file chiave consente di aggiungere una chiave per l'attivazione dell'applicazione.

Si riceve il file chiave tramite l'indirizzo e-mail specificato dopo l'acquisto di Kaspersky Security Center.

Per attivare l'applicazione utilizzando il file chiave, non è necessario connettersi ai server di attivazione di Kaspersky.

Se è stata selezionata questa opzione di attivazione, è possibile abilitare l'opzione **Distribuisci automaticamente la chiave di licenza ai dispositivi gestiti**.

Se questa opzione è abilitata, la chiave di licenza verrà distribuita automaticamente ai dispositivi gestiti.

Se questa opzione è disabilitata, è possibile distribuire la chiave di licenza ai dispositivi gestiti in un secondo momento, nella sezione **Operazioni** → **Licensing** → **Licenze di Kaspersky** del menu principale.

- Rimandando l'attivazione dell'applicazione

Se si sceglie di rimandare l'attivazione dell'applicazione, è possibile aggiungere una chiave di licenza in qualsiasi momento selezionando **Operazioni** → **Licensing**.

Se si utilizza Kaspersky Security Center distribuito da un'AMI a pagamento o per uno SKU con fatturazione mensile basato sull'utilizzo, non è possibile specificare un file chiave o immettere un codice.

Passaggio 9. Creazione di una configurazione della protezione di rete di base

È possibile esaminare un elenco dei criteri e delle attività creati.

Attendere il completamento della creazione di criteri e attività prima di procedere al passaggio successivo della procedura guidata.

Passaggio 10. Configurazione delle notifiche e-mail

Configurare l'invio di notifiche relative agli eventi registrati durante l'esecuzione delle applicazioni Kaspersky nei dispositivi client. Queste impostazioni verranno utilizzate come impostazioni predefinite per i criteri dell'applicazione.

Per configurare l'invio di notifiche relative agli eventi che si verificano nelle applicazioni Kaspersky, utilizzare le seguenti impostazioni:

- **Destinatari (indirizzi e-mail)**

  Gli indirizzi e-mail degli utenti a cui l'applicazione invierà le notifiche. È possibile immettere uno o più indirizzi; se si immette più di un indirizzo, separarli con un punto e virgola.

- **Indirizzo server SMTP**

  L'indirizzo o gli indirizzi dei server di posta dell'organizzazione.

  Se si immette più di un indirizzo, separarli con un punto e virgola. È possibile utilizzare i seguenti valori:

  - Indirizzo IPv4 o IPv6
  - Nome DNS del server SMTP

- **Porta server SMTP**

  Numero di porta di comunicazione del server SMTP. Se si utilizzano più server SMTP, la connessione a questi viene stabilita tramite la porta di comunicazione specificata. Il numero di porta predefinito è 25.

- **Usa autenticazione ESMTP**

  Abilita il supporto dell'autenticazione ESMTP. Quando la casella di controllo è selezionata, nei campi **Nome utente** e **Password** è possibile specificare le impostazioni per l'autenticazione ESMTP. Per impostazione predefinita, questa casella di controllo è deselezionata.

È possibile verificare le nuove impostazioni di notifica e-mail facendo clic sul pulsante **Invia messaggio di test**.

Passaggio 11. Chiusura dell'Avvio rapido guidato

Per chiudere la procedura guidata, fare clic sul pulsante **Fine**.

Dopo aver completato l'avvio rapido guidato è possibile eseguire la Distribuzione guidata della protezione per installare automaticamente le applicazioni anti-virus o Network Agent nei dispositivi della rete.

Distribuzione guidata della protezione

Per installare le applicazioni Kaspersky, è possibile utilizzare la Distribuzione guidata della protezione. La Distribuzione guidata della protezione consente l'installazione remota delle applicazioni con pacchetti di installazione creati appositamente o direttamente da un pacchetto di distribuzione.

La Distribuzione guidata della protezione esegue le seguenti operazioni:

- Download di un pacchetto di installazione per l'installazione dell'applicazione (se non è già stato creato). Il pacchetto di installazione è disponibile in **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**. È possibile utilizzare questo pacchetto di installazione per l'installazione dell'applicazione in futuro.

- Creazione ed esecuzione di un'attività di installazione remota per dispositivi specifici o per un gruppo di amministrazione. La nuova attività di installazione remota creata viene archiviata nella sezione **Attività**. È possibile avviare manualmente questa attività in un secondo momento. Il tipo di attività è **Installa l'applicazione in remoto**.

Se si desidera installare Network Agent nei dispositivi con sistema operativo SUSE Linux Enterprise Server 15, installare il pacchetto insserv-compat prima di configurare Network Agent.

Passaggio 1. Avvio della Distribuzione guidata della protezione

È possibile avviare manualmente la Distribuzione guidata della protezione in qualsiasi momento.

Per avviare manualmente la Distribuzione guidata della protezione:

Nella finestra principale dell'applicazione, passare a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Distribuzione guidata della protezione**.

Verrà avviata la Distribuzione guidata della protezione. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

Passaggio 2. Selezione del pacchetto di installazione

Selezionare il pacchetto di installazione dell'applicazione che si desidera installare.

Se il pacchetto di installazione dell'applicazione desiderata non è elencato, fare clic sul pulsante **Aggiungi** e quindi selezionare l'applicazione dall'elenco.

Passaggio 3. Selezione di un metodo per la distribuzione del file chiave o del codice di attivazione

Selezionare un metodo per la distribuzione del file chiave o del codice di attivazione:

- Non aggiungere la chiave di licenza al pacchetto di installazione

  La chiave viene distribuita automaticamente a tutti i dispositivi con cui è compatibile:
  - Se la distribuzione automatica è stata abilitata nelle proprietà della chiave.
  - Se l'attività **Aggiungi chiave** è stata creata.

- Aggiungi la chiave di licenza al pacchetto di installazione

La chiave verrà distribuita ai dispositivi insieme al pacchetto di installazione.

Non è consigliabile distribuire la chiave utilizzando questo metodo poiché i diritti di accesso condiviso in lettura sono abilitati nell'archivio dei pacchetti di installazione.

Se il pacchetto di installazione include già un file chiave o un codice di attivazione, questa finestra viene visualizzata, ma contiene solo le informazioni della chiave di licenza.

Passaggio 4. Selezione della versione di Network Agent

Se è stato selezionato il pacchetto di installazione di un'applicazione diversa da Network Agent, è necessario installare anche Network Agent, che connette l'applicazione con Kaspersky Security Center Administration Server.

Selezionare la versione più recente di Network Agent.

Passaggio 5. Selezione dei dispositivi

Specificare un elenco di dispositivi in cui verrà installata l'applicazione:

- **Installa nei dispositivi gestiti**

  Se questa opzione è selezionata, l'attività di installazione remota viene creata per un gruppo di dispositivi.

- **Selezionare i dispositivi per l'installazione**

  L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

Passaggio 6. Specificazione delle impostazioni dell'attività di installazione remota

Nella pagina **Impostazioni dell'attività di installazione remota** specificare le impostazioni per l'installazione remota dell'applicazione.

Nel gruppo di impostazioni **Forza il download del pacchetto di installazione** specificare la modalità di distribuzione dei file necessari per l'installazione dell'applicazione ai dispositivi client:

- **Utilizzando Network Agent**

Se questa opzione è abilitata, i pacchetti di installazione vengono distribuiti ai dispositivi client da Network Agent installato nei dispositivi client.

Se questa opzione è disabilitata, i pacchetti di installazione vengono distribuiti utilizzando gli strumenti del sistema operativo dei dispositivi client.

È consigliabile abilitare questa opzione se l'attività è stata assegnata a dispositivi in cui sono installati Network Agent.

Per impostazione predefinita, questa opzione è abilitata.

- **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**

  Se questa opzione è abilitata, i pacchetti di installazione verranno trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo tramite i punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete.

  Se l'opzione **Utilizzo di Network Agent** è abilitata, i file vengono inviati tramite gli strumenti del sistema operativo solo se gli strumenti di Network Agent non sono disponibili.

  Per impostazione predefinita, questa opzione è abilitata per le attività di installazione remota create in un Administration Server virtuale.

  L'unico modo per installare un'applicazione per Windows (incluso Network Agent per Windows) in un dispositivo in cui non è installato Network Agent consiste nell'utilizzare un punto di distribuzione basato su Windows. Pertanto, quando si installa un'applicazione Windows:

  - Selezionare questa opzione.
  - Assicurarsi che sia assegnato un punto di distribuzione per i dispositivi client di destinazione.
  - Assicurarsi che il punto di distribuzione sia basato su Windows.

Definire l'impostazione aggiuntiva:

Non reinstallare l'applicazione se è già installata

Se questa opzione è abilitata, l'applicazione selezionata non verrà reinstallata se è già stata installata nel dispositivo client.

Se questa opzione è disabilitata, l'applicazione verrà installata in ogni caso.

Per impostazione predefinita, questa opzione è abilitata.

Passaggio 7. Rimozione delle applicazioni incompatibili prima dell'installazione

Questo passaggio è presente solo se l'applicazione da distribuire risulta incompatibile con alcune altre applicazioni.

Selezionare l'opzione se si desidera che Kaspersky Security Center Linux rimuova automaticamente le applicazioni incompatibili con l'applicazione distribuita.

Viene visualizzato anche l'elenco delle applicazioni incompatibili.

Se non si seleziona questa opzione, l'applicazione verrà installata solo nei dispositivi in cui non sono presenti applicazioni incompatibili.

Passaggio 8. Spostamento dei dispositivi in Dispositivi gestiti

Specificare se i dispositivi devono essere spostati in un gruppo di amministrazione dopo l'installazione di Network Agent.

- **Non spostare i dispositivi**

  I dispositivi rimangono nei gruppi in cui si trovano attualmente. I dispositivi che non sono stati inseriti in alcun gruppo rimangono non assegnati.

- **Sposta i dispositivi non assegnati nel gruppo**

  I dispositivi vengono spostati nel gruppo di amministrazione selezionato.

L'opzione **Non spostare i dispositivi** è selezionata per impostazione predefinita. Per motivi di sicurezza, è consigliabile spostare i dispositivi manualmente.

Passaggio 9. Selezione degli account per l'accesso ai dispositivi

Se necessario, aggiungere gli account che verranno utilizzati per avviare l'attività di installazione remota:

- **Nessun account richiesto (Network Agent installato)**

  Se questa opzione è selezionata, non è necessario specificare un account con cui verrà eseguito il programma di installazione dell'applicazione. L'attività sarà eseguita tramite l'account con cui viene eseguito Administration Server.

  Se Network Agent non è stato installato nei dispositivi client, questa opzione non è disponibile.

- **Account richiesto (Network Agent non utilizzato)**

Selezionare questa opzione se Network Agent non è installato nei dispositivi a cui si assegna l'attività di installazione remota. In questo caso, è possibile specificare un account utente o un certificato SSH per installare l'applicazione.

- **Account locale**. Se questa opzione è selezionata, specificare l'account utente con cui verrà eseguito il programma di installazione dell'applicazione. Fare clic sul pulsante **Aggiungi**, selezionare **Account locale** e quindi specificare le credenziali dell'account utente.

  È possibile specificare più account utente, ad esempio se nessuno di essi dispone di tutti i diritti richiesti per tutti i dispositivi per cui si assegna l'attività. In questo caso, tutti gli account aggiunti vengono utilizzati per l'esecuzione dell'attività, consecutivamente, dall'alto in basso.

- **Certificato SSH**. Se si desidera installare un'applicazione in un dispositivo client basato su Linux, è possibile specificare un certificato SSH anziché un account utente. Fare clic sul pulsante **Aggiungi**, selezionare **Certificato SSH**, quindi specificare la chiave privata e quella pubblica del certificato.

  Per generare una chiave privata, è possibile utilizzare l'utilità ssh-keygen. Kaspersky Security Center Linux supporta il formato PEM delle chiavi private, ma l'utilità ssh-keygen genera chiavi SSH nel formato OPENSSH per impostazione predefinita. Il formato OPENSSH non è supportato da Kaspersky Security Center Linux. Per creare una chiave privata nel formato PEM supportato, aggiungere l'opzione -m PEM nel comando ssh-keygen. Ad esempio:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "< e-mail dell'utente >"
  ```

Passaggio 10. Avvio dell'installazione

Questo è il passaggio finale della procedura guidata. A questo punto, l'**Attività di installazione remota** è stata creata e configurata correttamente.

Per impostazione predefinita, l'opzione **Esegui l'attività al termine della procedura guidata** non è selezionata. Se si seleziona questa opzione, l'**Attività di installazione remota** verrà avviata immediatamente dopo il completamento della procedura guidata. Se non si seleziona questa opzione, l'**Attività di installazione remota** non verrà avviata. È possibile avviare manualmente questa attività in un secondo momento.

Fare clic su **OK** per completare il passaggio finale della Distribuzione guidata della protezione.

Upgrade di Kaspersky Security Center Linux

È possibile installare la versione 15 di Administration Server in un dispositivo in cui è installata una versione precedente di Administration Server (a partire dalla versione 13). Durante l'upgrade alla versione 15, tutti i dati e le impostazioni della versione precedente di Administration Server vengono mantenuti.

Prima di aggiornare Kaspersky Security Center Linux, assicurarsi di utilizzare le versioni del sistema operativo e del DBMS supportate dalla versione 15 di Administration Server. Se necessario, è possibile spostare Administration Server in un altro dispositivo con versioni successive del sistema operativo e del DBMS.

È possibile eseguire l'upgrade di una versione di Administration Server utilizzando uno dei seguenti metodi:

- Utilizzando il file di installazione di Kaspersky Security Center Linux
- Creando il backup dei dati di Administration Server, installando una nuova versione di Administration Server e ripristinando i dati di Administration Server dal backup

Durante l'aggiornamento, l'utilizzo simultaneo del DBMS da parte di Administration Server e di un'altra applicazione non è consentito.

Se la rete include diversi Administration Server, è necessario eseguire manualmente l'upgrade di ogni Server. Kaspersky Security Center Linux non supporta l'upgrade centralizzato.

Inoltre, è necessario eseguire l'upgrade di Kaspersky Security Center Web Console a una nuova versione.

Quando si aggiorna Kaspersky Security Center Linux da una versione precedente, tutti i plug-in installati delle applicazioni Kaspersky non vengono disinstallati. L'upgrade del plug-in di Administration Server e del plug-in di Network Agent vengono eseguiti automaticamente. Si consiglia di creare una copia di backup dei dati di Administration Server prima di avviare l'upgrade.

Upgrade di Kaspersky Security Center Linux utilizzando il file di installazione

Per eseguire l'upgrade di Administration Server da una versione precedente (a partire dalla versione 13) alla versione 15.2, è possibile installare una nuova versione su una precedente utilizzando il file di installazione di Kaspersky Security Center Linux.

Per eseguire l'upgrade di una versione precedente di Administration Server alla versione 15.2 utilizzando il file di installazione:

1. Scaricare il file di installazione di Kaspersky Security Center Linux con un pacchetto completo per la versione 15.2 dal sito Web di Kaspersky:
   - Per i dispositivi che eseguono un sistema operativo basato su RPM: ksc64—<numero versione>.x86_64.rpm
   - Per i dispositivi che eseguono un sistema operativo basato su Debian—ksc64_<numero versione>_amd64.deb
2. Aggiornare il pacchetto di installazione utilizzando uno strumento di gestione di pacchetti utilizzato nel proprio Administration Server. È ad esempio possibile utilizzare i seguenti comandi nel terminale della riga di comando con un account con privilegi di root:

- Per i dispositivi che eseguono un sistema operativo basato su RPM:
  `$ sudo yum install ./ksc64-<numero versione>.x86_64.rpm`

- Per i dispositivi che eseguono un sistema operativo basato su Debian:
  `$ sudo apt-get install ./ksc64_<numero versione>_amd64.deb`

Dopo aver eseguito il comando, viene creato lo script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl. Il relativo messaggio viene visualizzato nel terminale.

3. In un account con privilegi di root, eseguire lo script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl per configurare l'Administration Server aggiornato.

4. Leggere il Contratto di licenza e l'Informativa sulla privacy visualizzati nel terminale della riga di comando. Se si accettano tutti i termini del Contratto di licenza e dell'Informativa sulla privacy:

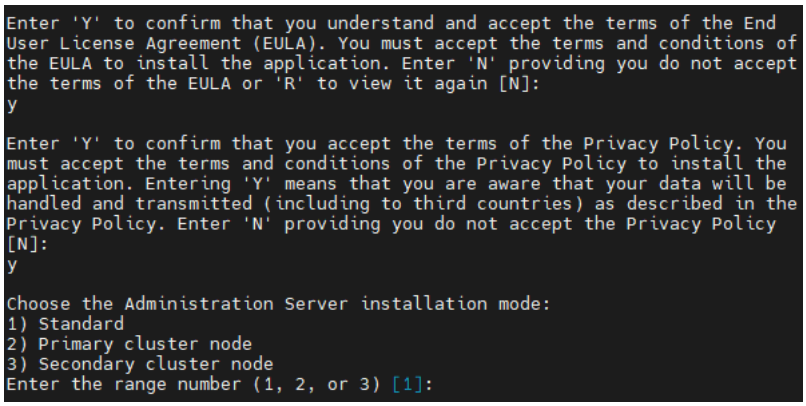
   a. Inserire 'Y' per confermare di aver letto, compreso e accettato i termini e le condizioni dell'EULA.

   b. Inserire nuovamente 'Y' per confermare di aver letto, compreso e accettato l'Informativa sulla privacy in cui viene descritta la gestione dei dati.

   L'installazione dell'applicazione nel dispositivo continuerà dopo aver inserito due volte 'Y'.

5. Immettere '1' per selezionare la modalità di installazione standard di Administration Server.

   L'immagine seguente mostra gli ultimi due passaggi.



Accettare i termini dell'EULA e l'Informativa sulla privacy e selezionare la modalità di installazione standard di Administration Server nel terminale della riga di comando

   Successivamente, lo script configura e termina l'aggiornamento di Administration Server. Durante l'aggiornamento, non è possibile modificare le impostazioni di Administration Server modificate prima dell'aggiornamento.

6. Per i dispositivi in cui è installata la versione precedente di Network Agent, creare ed eseguire l'attività di installazione remota per la nuova versione di Network Agent.

   Si consiglia di aggiornare Network Agent per Linux alla stessa versione di Kaspersky Security Center Linux.

   Al termine dell'attività di installazione remota, viene eseguito l'upgrade della versione di Network Agent.

Upgrade di Kaspersky Security Center Linux tramite backup

Per aggiornare Administration Server da una versione precedente (a partire dalla versione 13) alla versione 15, è possibile creare un backup dei dati di Administration Server e ripristinare questi dati dopo aver installato una nuova versione di Kaspersky Security Center Linux. Se si verificano problemi durante l'installazione, è possibile ripristinare la versione precedente di Administration Server utilizzando il backup dei dati di Administration Server creato prima dell'upgrade.

Per eseguire l'upgrade di una versione precedente di Administration Server alla versione 15 tramite il backup:

1. Prima dell'upgrade eseguire il backup dei dati di Administration Server con una versione precedente dell'applicazione.
2. Disinstallare la versione precedente di Kaspersky Security Center Linux.
3. Installare Kaspersky Security Center Linux versione 15 nell'Administration Server precedente.
4. Ripristinare i dati di Administration Server dal backup creato prima dell'upgrade.
5. Per i dispositivi in cui è installata la versione precedente di Network Agent, creare ed eseguire l'attività per l'installazione remota della nuova versione di Network Agent.

   Si consiglia di aggiornare Network Agent per Linux alla stessa versione di Kaspersky Security Center Linux.

   Al termine dell'attività di installazione remota, viene eseguito l'upgrade della versione di Network Agent.

Aggiornamento di Kaspersky Security Center Linux nei nodi del cluster di failover Kaspersky Security Center Linux

È possibile installare Administration Server versione 15 in ogni nodo del cluster di failover Kaspersky Security Center Linux in cui è installato l'Administration Server con una versione precedente (a partire dalla versione 14). Durante l'upgrade alla versione 15, tutti i dati e le impostazioni della versione precedente di Administration Server vengono mantenuti.

Se Kaspersky Security Center Linux è stato installato in precedenza nei dispositivi in locale, è inoltre possibile aggiornare Kaspersky Security Center Linux in questi dispositivi utilizzando il file di installazione o tramite backup.

Per aggiornare Kaspersky Security Center Linux nei nodi del cluster di failover Kaspersky Security Center Linux:

1. Scaricare il file di installazione di Kaspersky Security Center Linux con un pacchetto completo per la versione 15 dal sito Web di Kaspersky:
   - Per i dispositivi che eseguono un sistema operativo basato su RPM: ksc64—<numero versione>-<numero build>.x86_64.rpm
   - Per i dispositivi che eseguono un sistema operativo basato su Debian—ksc64_<numero versione>-<numero build>_amd64.deb
2. Arrestare il cluster.
3. Nel nodo attivo del cluster, aggiornare il pacchetto di installazione utilizzando uno strumento di gestione di pacchetti utilizzato nel proprio Administration Server.

È ad esempio possibile utilizzare i seguenti comandi nel terminale della riga di comando con un account con privilegi di root:

- Per i dispositivi che eseguono un sistema operativo basato su RPM:
  `$ sudo yum install ./ksc64-<numero versione>-<numero build>.x86_64.rpm`
- Per i dispositivi che eseguono un sistema operativo basato su Debian:
  `$ sudo apt-get install ./ksc64_<numero versione>-<numero build>_amd64.deb`

Dopo aver eseguito il comando, viene creato lo script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl. Il relativo messaggio viene visualizzato nel terminale.

4. In un account con privilegi di root, eseguire lo script /opt/kaspersky/ksc64/lib/bin/setup/postinstall.pl per configurare l'Administration Server aggiornato.

5. Leggere il Contratto di licenza e l'Informativa sulla privacy visualizzati nel terminale della riga di comando. Se si accettano tutti i termini del Contratto di licenza e dell'Informativa sulla privacy:

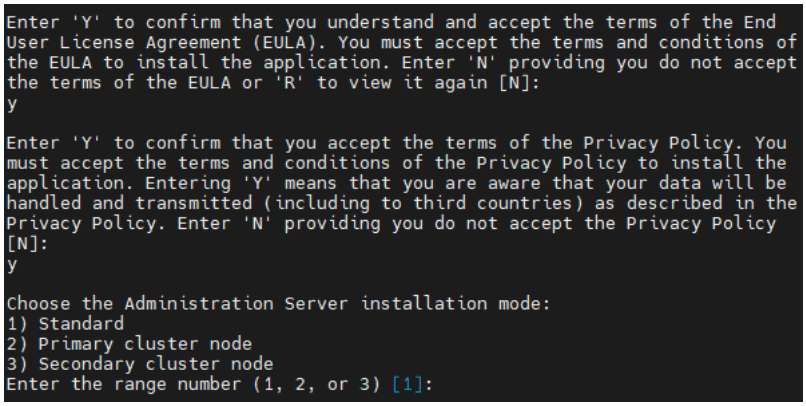
   a. Inserire 'Y' per confermare di aver letto, compreso e accettato i termini e le condizioni dell'EULA.

   b. Inserire nuovamente 'Y' per confermare di aver letto, compreso e accettato l'Informativa sulla privacy in cui viene descritta la gestione dei dati.

   L'installazione dell'applicazione nel dispositivo continuerà dopo aver inserito due volte 'Y'.

6. Selezionare il nodo in cui eseguire l'aggiornamento immettendo '2'.

   L'immagine seguente mostra gli ultimi due passaggi.



Accettare i termini dell'EULA e l'Informativa sulla privacy e selezionare la modalità di installazione nel terminale della riga di comando

   Successivamente, lo script configura e termina l'aggiornamento di Administration Server. Durante l'aggiornamento, non è possibile modificare le impostazioni di Administration Server modificate prima dell'aggiornamento.

7. Eseguire i passaggi 3-5 nel nodo passivo.

   Nel passaggio 6, immettere "3" per selezionare il nodo.

8. Avviare il cluster.

> Si noti che è possibile avviare il cluster in qualsiasi nodo. Se il cluster viene avviato nel nodo passivo, diventa il nodo attivo.

A questo punto, è stato installato Administration Server della versione più recente nei nodi del cluster di failover Kaspersky Security Center Linux.

Upgrade di Kaspersky Security Center Web Console

Questo articolo descrive come effettuare l'upgrade di Kaspersky Security Center Web Console Server (anche noto come Kaspersky Security Center Web Console) nei dispositivi in cui viene eseguito il sistema operativo Linux.

Se è necessario effettuare l'upgrade di Kaspersky Security Center Web Console su Astra Linux in modalità ambiente software chiuso, seguire le istruzioni specifiche per Astra Linux.

Utilizzare uno dei seguenti file di installazione che corrisponde alla distribuzione Linux installata nel proprio dispositivo:

- Per Debian—ksc-web-console-[numero_build].x86_64.deb
- Per i sistemi operativi basati su RPM—ksc-web-console-[numero_build].x86_64.rpm
- Per ALT 8 SP—ksc-web-console-[numero_build]-alt8p.x86_64.rpm

È possibile ottenere il file di installazione scaricandolo dal sito Web di Kaspersky.

Per eseguire l'upgrade di Kaspersky Security Center Web Console:

1. Verificare che il dispositivo in cui si desidera effettuare l'upgrade di Kaspersky Security Center Web Console esegua una delle distribuzioni Linux supportate.
2. Leggere e accettare il Contratto di licenza con l'utente finale (EULA). Se il kit di distribuzione di Kaspersky Security Center Linux non include un file TXT con il testo dell'EULA, è possibile scaricare il file dal sito Web di Kaspersky. Se non si accettano i termini del Contratto di licenza, non effettuare l'upgrade di Kaspersky Security Center Web Console utilizzando il file di installazione.
3. Utilizzare lo stesso file di risposta preparato prima dell'installazione di Kaspersky Security Center Web Console. Il nome del file di risposta è ksc-web-console-setup.json e il percorso del file è /etc/ksc-web-console-setup.json.

   Se il file di risposta non esiste, creare un nuovo file di risposta che contenga i parametri per la connessione di Kaspersky Security Center Web Console ad Administration Server. Denominare il file ksc-web-console-setup.json e posizionarlo nella directory /etc.

   Esempio di un file di risposta contenente il set minimo di parametri, nonché l'indirizzo e la porta predefiniti:

   ```
   {
     "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
   }
   ```

   Se si desidera effettuare l'upgrade di Kaspersky Security Center Web Console connesso all'Administration Server installato nei nodi del cluster di failover Kaspersky Security Center Linux, nel file di risposta specificare il parametro di installazione `attendibile` per consentire al cluster di failover Kaspersky Security Center Linux di connettersi a Kaspersky Security Center Web Console. Il valore stringa di questo parametro ha il seguente formato:

   ```
   "trusted": "indirizzo server|porta|percorso certificato|nome server"
   ```

   Specificare i componenti del parametro di installazione `trusted`:

- **Indirizzo di Administration Server**. Se una scheda di rete secondaria è stata creata durante la preparazione dei nodi del cluster, utilizzare l'indirizzo IP della scheda come indirizzo del cluster di failover Kaspersky Security Center Linux. In caso contrario, specificare l'indirizzo IP del sistema di bilanciamento del carico di terzi in uso.

- **Porta di Administration Server**. La porta OpenAPI utilizzata da Kaspersky Security Center Web Console per la connessione ad Administration Server (il valore predefinito è 13299).

- **Certificato di Administration Server**. Il certificato di Administration Server si trova nell'archivio dati condiviso del cluster di failover Kaspersky Security Center Linux. Il percorso predefinito del file del certificato: <cartella dati condivisa> \1093\cert\klserver.cer. Copiare il file del certificato dall'archivio dati condiviso nel dispositivo in cui si installa Kaspersky Security Center Web Console. Specificare il percorso locale del certificato di Administration Server.

- **Nome Administration Server**. Il nome del cluster di failover Kaspersky Security Center Linux che verrà visualizzato nella finestra di accesso di Kaspersky Security Center Web Console.

L'upgrade di Kaspersky Security Center Web Console non può essere effettuato utilizzando lo stesso file di installazione .rpm. Se si desidera modificare le impostazioni in un file di risposta e utilizzare questo file per reinstallare l'applicazione, è prima necessario rimuovere l'applicazione, quindi reinstallarla con il nuovo file di risposta.

4. In un account con privilegi di root, utilizzare la riga di comando per eseguire il file di installazione con estensione .deb o .rpm, a seconda della distribuzione Linux.

   Per eseguire l'upgrade da una versione precedente di Kaspersky Security Center Web Console, eseguire uno dei seguenti comandi:

   - Per i dispositivi che eseguono un sistema operativo basato su RPM:
     ```
     $ sudo rpm -Uvh --nodeps --force ksc-web-console-[numero_build].x86_64.rpm
     ```

   - Per i dispositivi che eseguono un sistema operativo basato su Debian:
     ```
     $ sudo dpkg -i ksc-web-console-[numero_build].x86_64.deb
     ```

   Verrà avviata la decompressione del file di installazione. Attendere il completamento dell'installazione.

5. Riavviare tutti i servizi Kaspersky Security Center Web Console eseguendo il comando seguente:
   ```
   $ sudo systemctl restart KSC*
   ```

Al termine dell'upgrade, è possibile utilizzare il browser per aprire e accedere a Kaspersky Security Center Web Console.

Upgrade di Kaspersky Security Center Web Console su Astra Linux in modalità ambiente software chiuso

Questa articolo descrive come effettuare l'upgrade di Kaspersky Security Center Web Console Server (anche noto come Kaspersky Security Center Web Console) nel sistema operativo Astra Linux Special Edition.

Per eseguire l'upgrade di Kaspersky Security Center Web Console:

1. Verificare che il dispositivo in cui si desidera effettuare l'upgrade di Kaspersky Security Center Web Console esegua una delle distribuzioni Linux supportate.

2. Leggere e accettare il Contratto di licenza con l'utente finale (EULA). Se il kit di distribuzione di Kaspersky Security Center Linux non include un file TXT con il testo dell'EULA, è possibile scaricare il file dal sito Web di Kaspersky. Se non si accettano i termini del Contratto di licenza, non effettuare l'upgrade di Kaspersky Security Center Web Console utilizzando il file di installazione.

3. Utilizzare lo stesso file di risposta preparato prima dell'installazione di Kaspersky Security Center Web Console. Il nome del file di risposta è ksc-web-console-setup.json e il percorso del file è /etc/ksc-web-console-setup.json.

   Se il file di risposta non esiste, creare un nuovo file di risposta che contenga i parametri per la connessione di Kaspersky Security Center Web Console ad Administration Server. Denominare il file ksc-web-console-setup.json e posizionarlo nella directory /etc.

   Esempio di un file di risposta contenente il set minimo di parametri, nonché l'indirizzo e la porta predefiniti:

   ```
   {
     "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. Assicurarsi che nel file `/etc/digsig/digsig_initramfs.conf` il parametro `DIGSIG_ELF_MODE` sia specificato come segue:

   ```
   DIGSIG_ELF_MODE=1
   ```

5. Assicurarsi che il pacchetto di compatibilità `astra-digsig-oldkeys` sia installato.

   Se questo pacchetto non è installato, eseguire il seguente comando:

   ```
   apt install astra-digsig-oldkeys
   ```

6. Creare una directory per la chiave dell'applicazione, se non esiste:

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

7. Posizionare la chiave dell'applicazione /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg nella directory creata nel passaggio precedente:

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

   > Se il kit di distribuzione di Kaspersky Security Center Linux non include la chiave dell'applicazione kaspersky_astra_pub_key.gpg, è possibile scaricarla facendo clic sul collegamento: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

8. Aggiornare i dischi RAM:

   ```
   update-initramfs -u -k all
   ```

   Riavviare il sistema.

9. In un account con privilegi di root, utilizzare la riga di comando per eseguire il file di installazione. È possibile ottenere il file di installazione scaricandolo dal sito Web di Kaspersky.

   Per eseguire l'upgrade da una versione precedente di Kaspersky Security Center Web Console, eseguire il comando seguente:

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

   Verrà avviata la decompressione del file di installazione. Attendere il completamento dell'installazione.

10. Riavviare tutti i servizi Kaspersky Security Center Web Console eseguendo il comando seguente:

```
$ sudo systemctl restart KSC*
```

Al termine dell'upgrade, è possibile utilizzare il browser per aprire e accedere a Kaspersky Security Center Web Console.

Migrazione a Kaspersky Security Center Linux

Seguendo questo scenario, è possibile trasferire la struttura del gruppo di amministrazione, inclusi i dispositivi gestiti e altri oggetti del gruppo (criteri, attività, attività globali, tag e selezioni di dispositivi) da Kaspersky Security Center Windows sotto la gestione di Kaspersky Security Center Linux.

Limitazioni:

- La migrazione è possibile solo da Kaspersky Security Center Windows versione 14.2 o successiva a Kaspersky Security Center Linux versione 15 o successiva.
- È possibile eseguire questo scenario solo utilizzando Kaspersky Security Center Web Console.

Prima di iniziare, scoprire di più sulle funzionalità e sui limiti di Kaspersky Security Center Linux:

- Differenze funzionali tra Kaspersky Security Center Windows e Kaspersky Security Center Linux
- Elenco delle applicazioni Kaspersky supportate da Kaspersky Security Center Linux

Passaggi

Lo scenario di migrazione procede per fasi:

1. **Scegliere un metodo di migrazione**

   Si esegue la migrazione a Kaspersky Security Center Linux tramite la Migrazione guidata. I passaggi della Migrazione guidata dipendono dalla disposizione gerarchica degli Administration Server di Kaspersky Security Center Windows e Kaspersky Security Center Linux:

   - Migrazione con l'utilizzo di una gerarchia di Administration Server

     Scegliere questa opzione se l'Administration Server di Kaspersky Security Center Windows funge da secondario rispetto all'Administration Server di Kaspersky Security Center Linux. Il processo di migrazione viene gestito e passa da un server all'altro all'interno di una singola istanza di Kaspersky Security Center Web Console. Se si preferisce questa opzione, è possibile disporre gli Administration Server in una gerarchia per semplificare la procedura di migrazione. A tale scopo, creare la gerarchia prima di avviare la migrazione.

   - Migrazione utilizzando un file di esportazione (archivio ZIP)

     Scegliere questa opzione se gli Administration Server di Kaspersky Security Center Windows e Kaspersky Security Center Linux non sono disposti in una gerarchia. Il processo di migrazione viene gestito con due istanze di Kaspersky Security Center Web Console: un'istanza per Kaspersky Security Center Windows e un'altra per Kaspersky Security Center Linux. In questo caso, si utilizzerà il file di esportazione creato e scaricato durante l'esportazione da Kaspersky Security Center Windows e si importerà questo file in Kaspersky Security Center Linux.

2. **Esportare i dati da Kaspersky Security Center Windows**

   Aprire Kaspersky Security Center Windows, quindi eseguire la Migrazione guidata.

3. **Importare i dati in Kaspersky Security Center Linux.**

   Continuare la Migrazione guidata per importare i dati esportati in Kaspersky Security Center Linux. Se i server sono organizzati in una gerarchia, l'importazione viene avviata automaticamente dopo un'esportazione riuscita all'interno della stessa procedura guidata. Se i server non sono organizzati in una gerarchia, continuare con la Migrazione guidata dopo essere passati a Kaspersky Security Center Linux.

4. **Eseguire azioni aggiuntive per trasferire manualmente oggetti e impostazioni da Kaspersky Security Center Windows a Kaspersky Security Center Linux (passaggio facoltativo)**

È inoltre possibile trasferire gli oggetti e le impostazioni che non possono essere trasferiti tramite la Migrazione guidata. Ad esempio, è possibile eseguire anche le seguenti operazioni:

- Trasferire le chiavi di licenza utilizzate da Administration Server e dalle applicazioni gestite
- Configurare le attività globali di Administration Server
- Configurare le impostazioni del criterio di Network Agent
- Creare pacchetti di installazione delle applicazioni
- Creare server virtuali
- Configurare regole di spostamento dei dispositivi
- Configurare regole per il tagging automatico dei dispositivi
- Creare categorie di applicazioni
- Assegnare e configurare punti di distribuzione

  Se si sposta un dispositivo che funge da punto di distribuzione su un altro Administration Server, i dispositivi inclusi nell'ambito del punto di distribuzione non vengono spostati automaticamente. È necessario spostare ogni dispositivo singolarmente. Se un punto di distribuzione funge da gateway, è necessario eseguire lo script `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl` in modo che il punto di distribuzione non svolga più la funzione di gateway.

5. **Spostare i dispositivi gestiti importati sotto la gestione di Kaspersky Security Center Linux**

   Per completare la migrazione, spostare i dispositivi gestiti importati sotto la gestione di Kaspersky Security Center Linux. È possibile procedere utilizzando uno dei seguenti metodi:

   - Tramite l'utilità klmover

     Utilizzare l'utilità klmover e specificare le impostazioni di connessione per il nuovo Administration Server.

   - Tramite l'attività *Change Administration Server*

     Creare un'attività *Change Administration Server*, specificare i dispositivi gestiti importati, il nuovo Administration Server e altre impostazioni dell'attività. Eseguire quindi l'attività per mettere i dispositivi gestiti sotto la gestione di Administration Server di Kaspersky Security Center Linux.

   - Tramite la rimozione (se già installato) e l'ulteriore installazione di Network Agent nei dispositivi gestiti

     Creare un nuovo pacchetto di installazione di Network Agent e specificare le impostazioni di connessione per il nuovo Administration Server nelle proprietà del pacchetto di installazione. Rimuovere Network Agent nei dispositivi gestiti importati, quindi utilizzare il pacchetto di installazione per installare Network Agent nei dispositivi gestiti importati tramite un'attività di installazione remota. È inoltre possibile creare e utilizzare un pacchetto di installazione indipendente per installare Network Agent in locale. Per ulteriori informazioni, vedere Passaggio dei dispositivi gestiti alla gestione di Kaspersky Security Center Linux.

6. **Aggiornare Network Agent all'ultima versione**

   Si consiglia di aggiornare Network Agent per Linux alla stessa versione di Kaspersky Security Center.

7. **Verificare che i dispositivi gestiti siano visibili nel nuovo Administration Server**

   In Kaspersky Security Center Linux Administration Server, aprire l'elenco dei dispositivi gestiti (**Risorse (dispositivi)** → DISPOSITIVI **Dispositivi gestiti**) e controllare i valori nelle colonne **Visibile**, **Network Agent installato** e **Ultima connessione ad Administration Server**.

Altri metodi di migrazione dei dati

Oltre alla migrazione guidata, esistono altri metodi per trasferire gli oggetti correnti, ma questi metodi consentono di trasferire solo criteri e attività:

- Esportare le attività da Kaspersky Security Center Windows, quindi importare le attività in Kaspersky Security Center Linux.
- Esportare i criteri specifici da Kaspersky Security Center Windows, quindi importare i criteri in Kaspersky Security Center Linux. I profili dei criteri correlati vengono esportati e importati insieme ai criteri selezionati.

Esportazione di oggetti di gruppo da Kaspersky Security Center Windows

La struttura dei gruppi di amministrazione della migrazione, inclusi i dispositivi gestiti e altri oggetti di gruppo da Kaspersky Security Center Windows a Kaspersky Security Center Linux, richiede che si selezionino prima i dati per l'esportazione e si crei un file di esportazione. Il file di esportazione contiene informazioni su tutti gli oggetti del gruppo di cui si desidera eseguire la migrazione. Questo file di esportazione verrà utilizzato per la successiva importazione in Kaspersky Security Center Linux.

È possibile esportare i seguenti oggetti:

- Attività e criteri delle applicazioni gestite
- Attività globali
- Selezioni dispositivi personalizzate
- Struttura di gruppi di amministrazione e dispositivi inclusi
- Tag assegnati ai dispositivi soggetti a migrazione

Prima di iniziare a esportare, leggere le informazioni generali sulla migrazione a Kaspersky Security Center Linux. Scegliere il metodo di migrazione, utilizzando o meno la gerarchia di Administration Server di Kaspersky Security Center Windows e Kaspersky Security Center Linux.

Per esportare i dispositivi gestiti e gli oggetti di gruppo correlati tramite la Migrazione guidata:

1. A seconda che gli Administration Server di Kaspersky Security Center Windows e Kaspersky Security Center Linux siano organizzati o meno in una gerarchia, effettuare una delle seguenti operazioni:
   - Se i server sono disposti in una gerarchia, aprire Kaspersky Security Center Web Console, quindi passare al server di Kaspersky Security Center Windows.
   - Se i server non sono disposti in una gerarchia, aprire Kaspersky Security Center Web Console connesso a Kaspersky Security Center Windows.
2. Nel menu principale, passare a **Operazioni** → **Migrazione**.
3. Selezionare **Migra a Kaspersky Security Center Linux o Kaspersky Single Management Platform** per avviare la procedura guidata e seguirne i passaggi.
4. Selezionare il gruppo o il sottogruppo di amministrazione da esportare. Accertarsi che il gruppo o il sottogruppo di amministrazione selezionato non contengano più di 10.000 dispositivi.
5. Selezionare le applicazioni gestite di cui esportare le attività e i criteri. Selezionare solo le applicazioni supportate da Kaspersky Security Center Linux. Gli oggetti delle applicazioni non supportate verranno

comunque esportati, ma non saranno utilizzabili.

6. Utilizzare i collegamenti a sinistra per selezionare le attività globali, le selezioni di dispositivi e i rapporti da esportare. Il collegamento **Oggetti del gruppo** consente di escludere ruoli personalizzati, utenti interni, gruppi di sicurezza e categorie di applicazioni personalizzate dall'esportazione.

Il file di esportazione (archivio ZIP) viene creato. A seconda che si esegua o meno la migrazione con il supporto della gerarchia di Administration Server, il file di esportazione viene salvato come segue:

- Se i server sono organizzati in una gerarchia, il file di esportazione viene salvato nella cartella temporanea in Kaspersky Security Center Web Console Server.
- Se i server non sono organizzati in una gerarchia, il file di esportazione viene scaricato nel dispositivo.

Per la migrazione con il supporto della gerarchia di Administration Server, l'importazione viene avviata automaticamente al termine dell'esportazione. Per la migrazione senza il supporto della gerarchia di Administration Server, è possibile importare manualmente il file di esportazione salvato in Kaspersky Security Center Linux.

Importazione del file di esportazione in Kaspersky Security Center Linux

Per trasferire le informazioni sui dispositivi gestiti, gli oggetti e le relative impostazioni esportate da Kaspersky Security Center Windows, è necessario importarle in Kaspersky Security Center Linux o Kaspersky Next XDR Expert.

Per importare i dispositivi gestiti e gli oggetti di gruppo correlati tramite la Migrazione guidata:

1. A seconda che gli Administration Server di Kaspersky Security Center Windows e Kaspersky Security Center Linux siano organizzati o meno in una gerarchia, effettuare una delle seguenti operazioni:
   - Se i server sono organizzati in una gerarchia, procedere al passaggio successivo della Migrazione guidata al termine dell'esportazione. L'importazione viene avviata automaticamente dopo un'esportazione riuscita all'interno di questa procedura guidata (vedere il passaggio 2 di questa istruzione).
   - Se i server non sono organizzati in una gerarchia:
     a. Aprire Kaspersky Security Center Web Console connesso a Kaspersky Security Center Linux o Kaspersky Next XDR Expert.
     b. Nel menu principale, passare a **Operazioni** → **Migrazione**.
     c. Selezionare il file di esportazione (archivio ZIP) creato e scaricato durante l' esportazione da Kaspersky Security Center Windows. Viene avviato il caricamento del file di esportazione.
2. Dopo che il file di esportazione è stato caricato correttamente, è possibile continuare l'importazione. Se si desidera specificare un altro file di esportazione, fare clic sul collegamento **Modifica**, quindi selezionare il file richiesto.
3. Viene visualizzata l'intera gerarchia dei gruppi di amministrazione di Kaspersky Security Center Linux.

   Selezionare la casella di controllo accanto al gruppo di amministrazione di destinazione in cui devono essere ripristinati gli oggetti del gruppo di amministrazione esportato (dispositivi gestiti, criteri, attività e altri oggetti del gruppo).
4. Viene avviata l'importazione degli oggetti di gruppo. Non è possibile ridurre a icona la Migrazione guidata ed eseguire operazioni simultanee durante l'importazione. Attendere finché le icone di aggiornamento (🔄) accanto

a tutti gli elementi nell'elenco di oggetti non vengono sostituite con segni di spunta verdi (✓). A questo punto, l'importazione è stata completata.

5. Al termine dell'importazione, la struttura esportata dei gruppi di amministrazione, inclusi i dettagli dei dispositivi, viene visualizzata sotto il gruppo di amministrazione di destinazione selezionato. Se il nome dell'oggetto ripristinato è identico al nome di un oggetto esistente, all'oggetto ripristinato viene aggiunto un suffisso incrementale.

> Se in un'attività migrata sono specificati i dettagli dell'account con cui viene eseguita l'attività, è necessario aprire l'attività e immettere nuovamente la password al termine dell'importazione.

Se l'importazione è stata completata con un errore, è possibile eseguire una delle seguenti operazioni:

- Per la migrazione con il supporto della gerarchia di Administration Server, è possibile iniziare a importare nuovamente il file di esportazione.
- Per la migrazione senza il supporto della gerarchia di Administration Server, è possibile avviare la Migrazione guidata per selezionare un altro file di esportazione e quindi importarlo di nuovo.

È possibile verificare se gli oggetti del gruppo inclusi nell'ambito di esportazione sono stati importati correttamente in Kaspersky Security Center Linux. A tale scopo, accedere alla sezione **Risorse (dispositivi)** e verificare che gli oggetti importati vengano visualizzati nelle sottosezioni corrispondenti.

Si noti che i dispositivi gestiti importati vengono visualizzati nella sottosezione **Dispositivi gestiti**, ma sono invisibili nella rete e Network Agent non è installato e in esecuzione su di essi (il valore *No* nelle colonne **Visibile**, **Network Agent installato** e **Network Agent è in esecuzione**).

Per completare la migrazione, è necessario impostare i dispositivi gestiti in modo che siano gestiti da Kaspersky Security Center Linux.

Passaggio dei dispositivi gestiti alla gestione di Kaspersky Security Center Linux

Dopo aver importato correttamente le informazioni sui dispositivi gestiti, gli oggetti e le relative impostazioni in Kaspersky Security Center Linux, è necessario impostare i dispositivi gestiti in modo che siano gestiti da Kaspersky Security Center Linux per completare la migrazione.

È possibile spostare i dispositivi gestiti in Kaspersky Security Center Linux in uno dei seguenti metodi:

- Utilizzando l'utilità klmover.
- Utilizzando l'attività *Change Administration Server*.
- Installazione di Network Agent nei dispositivi gestiti tramite un'attività di installazione remota.

Per impostare i dispositivi gestiti in modo che siano gestiti da Kaspersky Security Center Linux installando Network Agent:

1. Rimuovere Network Agent nei dispositivi gestiti importati di cui verrà eseguito il passaggio durante la gestione di Kaspersky Security Center Linux.
2. Passare ad Administration Server di Kaspersky Security Center Windows.

3. Accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**, quindi aprire le proprietà di un pacchetto di installazione esistente di Network Agent.

   Se il pacchetto di installazione di Network Agent non è presente nell'elenco dei pacchetti, scaricarne uno nuovo.

   È inoltre possibile creare e utilizzare un pacchetto di installazione indipendente per installare Network Agent in locale.

4. Nella scheda **Impostazioni**, selezionare la sezione **Connessione**. Specificare le impostazioni di connessione di Administration Server di Kaspersky Security Center Linux.

5. Creare un'attività di installazione remota per i dispositivi gestiti importati, quindi specificare il pacchetto di installazione di Network Agent riconfigurato.

   È possibile installare Network Agent tramite Administration Server di Kaspersky Security Center Windows o tramite un dispositivo basato su Windows che funge da punto di distribuzione. Se si utilizza Administration Server, abilitare l'opzione **Utilizzando le risorse del sistema operativo tramite Administration Server**. Se si utilizza un punto di distribuzione, abilitare l'opzione **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**.

6. Eseguire l'attività di installazione remota.

Al termine dell'attività di installazione remota, accedere ad Administration Server di Kaspersky Security Center Linux e verificare che i dispositivi gestiti siano visibili nella rete e che Network Agent sia installato e in esecuzione (il valore *Sì* nelle colonne **Visibile**, **Network Agent installato** e **Network Agent è in esecuzione**).

Configurazione di Administration Server

Questa sezione descrive il processo di configurazione e le proprietà di Kaspersky Security Center Administration Server.

Configurazione della connessione di Kaspersky Security Center Web Console ad Administration Server

Per impostare le porte di connessione di Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Porte di connessione**.

L'applicazione visualizzerà le impostazioni di connessione principali del server selezionato.

Configurazione di una lista di indirizzi IP consentiti per connettersi a Kaspersky Security Center Linux

Per impostazione predefinita, le connessioni a Kaspersky Security Center Linux sono consentite da qualsiasi dispositivo. Ad esempio, è possibile installare Kaspersky Security Center Web Console Server su qualsiasi dispositivo che soddisfi i requisiti e Kaspersky Security Center Web Console Server comunicherà con Kaspersky Security Center Linux. Tuttavia, è possibile configurare Administration Server in modo che le connessioni siano consentite solo dai dispositivi con gli indirizzi IP specificati. In questo caso, se un intruso tenta di connettersi a Kaspersky Security Center Linux tramite Kaspersky Security Center Web Console Server installato su un dispositivo non incluso nella lista consentiti, non sarà in grado di accedere a Kaspersky Security Center Linux.

L'indirizzo IP viene verificato quando un utente accede a Kaspersky Security Center Linux o esegue un'applicazione che interagisce con Administration Server tramite Kaspersky Security Center Linux OpenAPI. In questo momento, un'applicazione su un dispositivo tenta di stabilire una connessione con Administration Server. Se l'indirizzo IP del dispositivo non è presente nella lista consentiti, si verifica un errore di autenticazione e l'evento KLAUD_EV_SERVERCONNECT informa l'utente che non è stata stabilita una connessione con Administration Server.

Requisiti per una lista di indirizzi IP consentiti

Gli indirizzi IP vengono verificati solo quando le seguenti applicazioni tentano di connettersi ad Administration Server:

- Kaspersky Security Center Web Console Server

  Se si accede a Kaspersky Security Center Linux tramite Kaspersky Security Center Web Console, è possibile configurare un firewall nel dispositivo in cui è installato Kaspersky Security Center Web Console Server utilizzando le modalità standard del sistema operativo. Se quindi qualcuno tenta di accedere a Kaspersky Security Center Linux in un dispositivo e Kaspersky Security Center Web Console Server è installato in un altro dispositivo, un firewall aiuta a prevenire l'interferenza di intrusi.

- Applicazioni che interagiscono con Administration Server tramite oggetti di automazione klakaut
- Applicazioni che interagiscono con Administration Server tramite OpenAPI, come Kaspersky Anti Targeted Attack Platform o Kaspersky Security for Virtualization

Specificare quindi gli indirizzi dei dispositivi in cui sono installate le applicazioni sopra elencate.

È possibile impostare indirizzi IPv4 e IPv6. Non è possibile specificare intervalli di indirizzi IP.

Come stabilire una lista di indirizzi IP consentiti

Se non è stata impostata una lista consentiti in precedenza, seguire le istruzioni di seguito.

Per stabilire una lista di indirizzi IP consentiti per accedere a Kaspersky Security Center Linux:

1. Nel dispositivo Administration Server eseguire il prompt dei comandi con un account che disponga dei diritti di amministratore.
2. Modificare la directory corrente nella cartella di installazione di Kaspersky Security Center Linux (in genere, /opt/kaspersky/ksc64/sbin).
3. Immettere il seguente comando nell'account root:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v “<Indirizzi IP>" -t s`

   Specificare gli indirizzi IP che soddisfano i requisiti sopra elencati. I diversi indirizzi IP devono essere separati da un punto e virgola.

   Esempio di come consentire a un solo dispositivo di connettersi ad Administration Server:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Esempio di come consentire a più dispositivi di connettersi ad Administration Server:

   `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. Riavviare il servizio Administration Server.

È possibile verificare se è stata configurata correttamente la lista di indirizzi IP consentiti nel Registro eventi Syslog in Administration Server.

Come modificare una lista di indirizzi IP consentiti

È possibile modificare una lista consentiti seguendo i passaggi previsti per la relativa creazione. A tale scopo, eseguire lo stesso comando e specificare una nuova lista consentiti:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v “<Indirizzi IP>" -t s
```

Se si desidera eliminare alcuni indirizzi IP dalla lista consentiti, riscriverla. Ad esempio, la lista consentiti include i seguenti indirizzi IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. Si desidera eliminare l'indirizzo IP 198.51.100.0. A tale scopo, immettere il seguente comando nel prompt dei comandi:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Non dimenticare di riavviare il servizio Administration Server.

Come reimpostare una lista di indirizzi IP consentiti configurata

Per reimpostare una lista di indirizzi IP consentiti già configurata:

1. Immettere il seguente comando al prompt dei comandi sotto l'account root:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`
2. Riavviare il servizio Administration Server.

Successivamente, gli indirizzi IP non vengono più verificati.

Configurazione delle impostazioni di accesso a Internet per Administration Server

È necessario configurare l'accesso a Internet per utilizzare Kaspersky Security Network e per scaricare gli aggiornamenti dei database anti-virus per Kaspersky Security Center Linux e le applicazioni Kaspersky gestite.

Per specificare le impostazioni di accesso a Internet per Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server.
   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Generale** selezionare la sezione **Configurazione dell'accesso a Internet**.
3. Se si desidera utilizzare un server proxy durante la connessione a Internet, abilitare l'opzione **Usa server proxy**. Se questa opzione è abilitata, i campi sono disponibili per l'immissione delle impostazioni. Specificare le seguenti impostazioni per la connessione a un server proxy:

   - **Indirizzo**

     Indirizzo del server proxy utilizzato per la connessione di Kaspersky Security Center Linux a Internet.

   - **Numero di porta**

     Numero della porta utilizzata per stabilire la connessione al proxy di Kaspersky Security Center Linux.

   - **Ignora il server proxy per gli indirizzi locali**

     Non verrà utilizzato alcun server proxy per la connessione ai dispositivi dalla rete locale.

   - **Autenticazione server proxy**

     Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

     Questo campo di immissione è disponibile se la casella di controllo **Usa server proxy** è selezionata.

- **Nome utente**

  Account utente con il quale è stata stabilita la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

- **Password**

  Password impostata dall'utente di cui è stato utilizzato l'account per stabilire la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

  Per visualizzare la password immessa, tenere premuto il pulsante **Mostra** per il tempo necessario.

È inoltre possibile configurare l'accesso a Internet utilizzando l'Avvio rapido guidato.

Gerarchia di Administration Server

Alcune società clienti, ad esempio MSP, possono eseguire più Administration Server. Poiché può essere scomodo amministrare più Administration Server distinti, è possibile applicare una gerarchia. In una gerarchia, un Administration Server basato su Linux può fungere sia da server primario che da server secondario. Il server primario basato su Linux può gestire sia i server secondari basati su Linux che quelli basati su Windows. Un server primario basato su Windows può gestire un server secondario basato su Linux.

Una configurazione "primario/secondario" per due Administration Server fornisce le seguenti opzioni:

- Un Administration Server secondario eredita i criteri, le attività, i ruoli utente e i pacchetti di installazione dall'Administration Server primario, evitando così la duplicazione delle impostazioni.
- Le selezioni di dispositivi nell'Administration Server primario possono includere i dispositivi degli Administration Server secondari.
- I rapporti nell'Administration Server primario possono contenere dati (incluse informazioni dettagliate) ottenuti dagli Administration Server secondari.
- È possibile utilizzare un Administration Server primario come sorgente degli aggiornamenti per l'Administration Server secondario.

L'Administration Server primario riceve i dati solo dagli Administration Server secondari non virtuali nell'ambito delle opzioni elencate sopra. Questa limitazione non si applica agli Administration Server virtuali, che condividono il database con l'Administration Server primario.

Creazione di una gerarchia di Administration Server: l'aggiunta un Administration Server secondario

In una gerarchia, un Administration Server basato su Linux può fungere sia da server primario che da server secondario. Il server primario basato su Linux può gestire sia i server secondari basati su Linux che quelli basati su Windows. Un server primario basato su Windows può gestire un server secondario basato su Linux.

Aggiunta di un Administration Server secondario (eseguita sul futuro Administration Server primario)

È possibile aggiungere un Administration Server come Administration Server secondario, configurando una gerarchia "primario/secondario".

Per aggiungere un Administration Server secondario disponibile per la connessione tramite Kaspersky Security Center Web Console:

1. Verificare che la porta 13000 del futuro Administration Server primario sia disponibile per la ricezione delle connessioni dagli Administration Server secondari.
2. Nel futuro Administration Server primario, fare clic sull'icona delle impostazioni ( ).
3. Nella pagina delle proprietà visualizzata fare clic sulla scheda **Administration Server**.
4. Selezionare la casella di controllo accanto al nome del gruppo di amministrazione a cui si desidera aggiungere l'Administration Server.
5. Nella riga del menu fare clic su **Connetti Administration Server secondario**.

   Verrà avviata l'Aggiunta guidata Administration Server secondari. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
6. Compilare i seguenti campi:

   - Nome visualizzato dell'Administration Server secondario

     Un nome con cui l'Administration Server secondario verrà visualizzato nella gerarchia. Se si desidera, è possibile immettere l'indirizzo IP come nome, oppure è possibile utilizzare un nome come "Server secondario per il gruppo 1".

   - Indirizzo dell'Administration Server secondario (facoltativo)

     Specificare l'indirizzo IP o il nome di dominio dell'Administration Server secondario.

     Questo parametro è obbligatorio se l'opzione **Connetti l'Administration Server primario all'Administration Server secondario nella rete perimetrale** è abilitata.

   - Porta SSL Administration Server

     Specificare il numero della porta SSL nell'Administration Server primario. Il numero di porta predefinito è 13000.

   - Porta API Administration Server

     Specificare il numero della porta nell'Administration Server primario per la ricezione delle connessioni tramite OpenAPI. Il numero di porta predefinito è 13299.

   - Connetti l'Administration Server primario all'Administration Server secondario nella rete perimetrale

     Selezionare questa opzione se l'Administration Server secondario si trova in una rete perimetrale (DMZ).

     Se questa opzione è selezionata, l'Administration Server primario avvia la connessione all'Administration Server secondario. In caso contrario, l'Administration Server secondario avvia una connessione con l'Administration Server primario.

- Usa server proxy

  Selezionare questa opzione se si utilizza un server proxy per la connessione all'Administration Server secondario.

  In tal caso, è inoltre necessario specificare le seguenti impostazioni del server proxy:

  - **Indirizzo**
  - **Nome utente**
  - **Password**

7. Specificare le impostazioni di connessione:

   - Immettere l'indirizzo del futuro Administration Server primario.
   - Se il futuro Administration Server secondario utilizza un server proxy, immettere l'indirizzo del server proxy e le credenziali dell'utente per connettersi al server proxy.

8. Immettere le credenziali dell'utente che dispone dei diritti di accesso sul futuro Administration Server secondario.

   Assicurarsi che la verifica in due passaggi sia disabilitata per l'account specificato. Se la verifica in due passaggi è abilitata per questo account, è possibile creare la gerarchia solo dal futuro Administration Server secondario (consultare le istruzioni di seguito). Questo è un problema noto.

Se le impostazioni di connessione sono corrette, viene stabilita la connessione con il futuro Administration Server secondario e viene costruita la gerarchia "primario/secondario". Se la connessione non è riuscita, verificare le impostazioni di connessione o specificare il certificato del futuro Administration Server secondario manualmente.

La connessione potrebbe anche non riuscire perché il futuro Administration Server secondario è autenticato con un certificato autofirmato generato automaticamente da Kaspersky Security Center Linux. Di conseguenza, il browser potrebbe bloccare il download del certificato autofirmato. Se è questo il caso, è possibile eseguire una delle seguenti operazioni:

- Per il futuro Administration Server secondario, creare un certificato attendibile nella propria infrastruttura e che soddisfi i requisiti dei certificati personalizzati.
- Aggiungere il certificato autofirmato del futuro Administration Server secondario all'elenco dei certificati attendibili del browser. È consigliabile utilizzare questa opzione solo se non è possibile creare un certificato personalizzato. Per informazioni sull'aggiunta di un certificato all'elenco dei certificati attendibili, fare riferimento alla documentazione del browser in uso.

Al termine della procedura guidata, verrà creata la gerarchia "primario/secondario". La connessione tra l'Administration Server primario e quello secondario viene stabilita tramite la porta 13000. Le attività e i criteri dall'Administration Server primario vengono ricevuti e applicati. L'Administration Server secondario viene visualizzato nell'Administration Server primario, nel gruppo di amministrazione a cui è stato aggiunto.

Aggiunta di un Administration Server secondario (eseguita sul futuro Administration Server secondario)

Se non è possibile connettersi al futuro Administration Server secondario (ad esempio, perché temporaneamente disconnesso o non disponibile o perché il file del certificato dell'Administration Server secondario è autofirmato), è comunque possibile aggiungere un Administration Server secondario.

Per aggiungere come secondario un Administration Server non disponibile per la connessione tramite Kaspersky Security Center Web Console:

1. Inviare il file del certificato del futuro Administration Server primario all'amministratore di sistema dell'ufficio in cui si trova il futuro Administration Server secondario. È ad esempio possibile scrivere il file su un dispositivo esterno, come un'unità flash, o inviarlo via e-mail.

   Il file del certificato si trova nel futuro Administration Server primario, in /var/opt/kaspersky/klnagent_srv/1093/cert/.

2. Richiedere all'amministratore di sistema responsabile del futuro Administration Server secondario di eseguire le seguenti operazioni:

   a. Fare clic sull'icona delle impostazioni ( ).

   b. Nella pagina delle proprietà visualizzata passare alla sezione **Gerarchia di Administration Server** della scheda **Generale**.

   c. Selezionare l'opzione **Questo Administration Server è secondario nella gerarchia**.

   d. Nel campo **Indirizzo Administration Server primario** immettere il nome della rete del futuro Administration Server primario.

   e. Selezionare il file precedentemente salvato con il certificato del futuro Administration Server primario facendo clic su **Sfoglia**.

   f. Se necessario, selezionare la casella di controllo **Connetti l'Administration Server primario all'Administration Server secondario nella rete perimetrale**.

   g. Se la connessione al futuro Administration Server primario viene eseguita tramite un server proxy, selezionare l'opzione **Usa server proxy** e specificare le impostazioni di connessione.

   h. Fare clic su **Salva**.

Verrà creata la gerarchia "primario/secondario". L'Administration Server primario inizia a ricevere la connessione dall'Administration Server secondario tramite la porta 13000. Le attività e i criteri dall'Administration Server primario vengono ricevuti e applicati. L'Administration Server secondario viene visualizzato nell'Administration Server primario, nel gruppo di amministrazione a cui è stato aggiunto.

Visualizzazione dell'elenco degli Administration Server secondari

Per visualizzare l'elenco degli Administration Server secondari (inclusi quelli virtuali):

Nel menu principale, fare clic sul nome di Administration Server, accanto all'icona delle impostazioni ( ).

Viene visualizzato l'elenco a discesa degli Administration Server secondari (inclusi quelli virtuali).

È possibile passare a uno di questi Administration Server facendo clic sul relativo nome.

Vengono visualizzati anche i gruppi di amministrazione, che sono però disattivati e non disponibili per la gestione in questo menu.

Se si è connessi all'Administration Server primario in Kaspersky Security Center Web Console e non è possibile connettersi a un Administration Server virtuale gestito da un Administration Server secondario, è possibile utilizzare uno dei seguenti modi:

- **Modificare l'installazione esistente di Kaspersky Security Center Web Console per aggiungere il server secondario all'elenco degli Administration Server attendibili**. Sarà quindi possibile connettersi all'Administration Server virtuale in Kaspersky Security Center Web Console.

  1. Nel dispositivo in cui è installato Kaspersky Security Center Web Console, eseguire il file di installazione di Kaspersky Security Center Web Console corrispondente alla distribuzione Linux installata nel dispositivo con un account dotato di privilegi amministrativi.

     Verrà avviata l'Installazione guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

  2. Selezionare l'opzione **Upgrade**.

  3. Nel passaggio **Tipo di modifica** selezionare l'opzione **Modifica impostazioni di connessione**.

  4. Nel passaggio **Administration Server attendibili**, aggiungere l'Administration Server secondario richiesto.

  5. Nell'ultimo passaggio fare clic su **Modifica** per applicare le nuove impostazioni.

  6. Al termine della riconfigurazione dell'applicazione, fare clic sul pulsante **Fine**.

- Utilizzare Kaspersky Security Center Web Console per connettersi direttamente all'Administration Server secondario in cui è stato creato il server virtuale. Sarà quindi possibile passare all'Administration Server virtuale in Kaspersky Security Center Web Console.

Gestione di Administration Server virtuali

Questa sezione descrive le seguenti azioni per gestire Administration Server virtuali:

- Creare Administration Server virtuali
- Abilitare e disabilitare Administration Server virtuali
- Assegnare un amministratore per un Administration Server virtuale
- Modificare Administration Server per i dispositivi client
- Eliminare Administration Server virtuali

Creazione di un Administration Server virtuale

È possibile creare Administration Server virtuali e aggiungerli ai gruppi di amministrazione.

Quando si crea un Administration Server virtuale, eredita l'elenco di utenti e tutti i diritti utente dell'Administration Server primario. Se un utente dispone dei diritti di accesso al server primario, ha anche i diritti di accesso al server virtuale. Dopo la creazione, si configurano i diritti di accesso ai server in modo indipendente.

Per creare e aggiungere un Administration Server virtuale:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

2. Nella pagina visualizzata passare alla scheda **Administration Server**.

3. Selezionare il gruppo di amministrazione a cui si desidera aggiungere un Administration Server virtuale. L'Administration Server virtuale gestirà i dispositivi del gruppo selezionato (compresi i sottogruppi).

4. Nella riga del menu fare clic su **Nuovo Administration Server virtuale**.

5. Nella pagina visualizzata definire le proprietà del nuovo Administration Server virtuale:

   - **Nome Administration Server virtuale**.

   - **Indirizzo connessione Administration Server**

     È possibile specificare il nome o l'indirizzo IP di Administration Server.

   Nell'elenco degli utenti selezionare l'amministratore dell'Administration Server virtuale. Se si desidera, è possibile modificare uno degli account esistenti prima di assegnargli il ruolo di amministratore o creare un nuovo account utente.

6. Fare clic su **Salva**.

   Il nuovo Administration Server virtuale verrà creato, aggiunto al gruppo di amministrazione e visualizzato nella scheda **Administration Server**.

Se si è connessi all'Administration Server primario in Kaspersky Security Center Web Console e non è possibile connettersi a un Administration Server virtuale gestito da un Administration Server secondario, è possibile utilizzare uno dei seguenti modi:

- **Modificare l'installazione esistente di Kaspersky Security Center Web Console per aggiungere il server secondario all'elenco degli Administration Server attendibili**. Sarà quindi possibile connettersi all'Administration Server virtuale in Kaspersky Security Center Web Console.

1. Nel dispositivo in cui è installato Kaspersky Security Center Web Console, eseguire il file di installazione di Kaspersky Security Center Web Console corrispondente alla distribuzione Linux installata nel dispositivo con un account dotato di privilegi amministrativi.

   Verrà avviata l'Installazione guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Selezionare l'opzione **Upgrade**.

3. Nel passaggio **Tipo di modifica** selezionare l'opzione **Modifica impostazioni di connessione**.

4. Nel passaggio **Administration Server attendibili**, aggiungere l'Administration Server secondario richiesto.

5. Nell'ultimo passaggio fare clic su **Modifica** per applicare le nuove impostazioni.

6. Al termine della riconfigurazione dell'applicazione, fare clic sul pulsante **Fine**.

- Utilizzare Kaspersky Security Center Web Console per connettersi direttamente all'Administration Server secondario in cui è stato creato il server virtuale. Sarà quindi possibile passare all'Administration Server virtuale in Kaspersky Security Center Web Console.

Abilitazione e disabilitazione di un Administration Server virtuale

Quando si crea un nuovo Administration Server virtuale, questo viene abilitato per impostazione predefinita. È possibile disabilitarlo o abilitarlo nuovamente in qualsiasi momento. La disabilitazione o l'abilitazione di un Administration Server virtuale equivale alla disattivazione o all'attivazione di un Administration Server fisico.

Per abilitare o disabilitare un Administration Server virtuale:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

2. Nella pagina visualizzata passare alla scheda **Administration Server**.

3. Selezionare l'Administration Server virtuale che si desidera abilitare o disabilitare.

4. Nella riga del menu fare clic sul pulsante **Abilita/disabilita l'Administration Server virtuale**.

   Lo stato dell'Administration Server virtuale viene modificato in abilitato o disabilitato, a seconda del suo stato precedente. Viene visualizzato lo stato aggiornato accanto al nome dell'Administration Server.

Assegnazione di un amministratore per un Administration Server virtuale

Quando si utilizzano Administration Server virtuali nell'organizzazione, è consigliabile assegnare un amministratore dedicato per ciascun Administration Server virtuale. Questo potrebbe ad esempio essere utile quando si creano Administration Server virtuali per gestire uffici o reparti separati della propria organizzazione oppure se si è un provider MSP e si gestiscono i tenant tramite Administration Server virtuali.

Quando si crea un Administration Server virtuale, eredita l'elenco di utenti e tutti i diritti utente dell'Administration Server primario. Se un utente dispone dei diritti di accesso al server primario, ha anche i diritti di accesso al server virtuale. Dopo la creazione, si configurano i diritti di accesso ai server in modo indipendente. Se si desidera assegnare un amministratore solo per un Administration Server virtuale, accertarsi che l'amministratore non disponga dei diritti di accesso nell'Administration Server primario.

Si assegna un amministratore per un Administration Server virtuale concedendo all'amministratore i diritti di accesso all'Administration Server virtuale. È possibile concedere i diritti di accesso necessari in uno dei seguenti modi:

- Configurare manualmente i diritti di accesso per l'amministratore
- Assegnare uno o più ruoli utente per l'amministratore

Per accedere a Kaspersky Security Center Web Console, un amministratore di un Administration Server virtuale specifica il nome, il nome utente e la password dell'Administration Server virtuale. Kaspersky Security Center Web Console autentica l'amministratore e apre l'Administration Server virtuale per il quale l'amministratore dispone dei diritti di accesso. L'amministratore non può passare da un Administration Server all'altro.

Prerequisiti

Prima di iniziare, assicurarsi che vengano soddisfatte le seguenti condizioni:

- L'Administration Server virtuale è stato creato.
- Nell'Administration Server primario è stato creato un account per l'amministratore che si desidera assegnare per l'Administration Server virtuale.
- L'utente dispone del diritto **Modifica elenchi di controllo degli accessi agli oggetti** nell'area funzionale **Caratteristiche generali → Autorizzazioni utente**.

Configurazione manuale dei diritti di accesso

Per assegnare un amministratore per un Administration Server virtuale:

1. Nella menu principale, passare all'Administration Server virtuale desiderato:
   a. Fare clic sull'icona a forma di freccia di espansione ( ) a destra del nome corrente dell'Administration Server.
   b. Selezionare l'Administration Server desiderato.
2. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome di Administration Server.
   Verrà visualizzata la finestra delle proprietà di Administration Server.
3. Nella scheda **Diritti di accesso**, fare clic sul pulsante **Aggiungi**.
   Viene visualizzato un elenco unificato di utenti dell'Administration Server primario e dell'Administration Server virtuale corrente.
4. Nell'elenco di utenti selezionare l'account dell'amministratore che si desidera assegnare per l'Administration Server virtuale, quindi fare clic sul pulsante **OK**.
   L'applicazione aggiunge l'utente selezionato all'elenco utenti nella scheda **Diritti di accesso**.
5. Selezionare la casella di controllo accanto all'account aggiunto, quindi fare clic sul pulsante **Diritti di accesso**.

6. Configurare i diritti che l'amministratore avrà sull'Administration Server virtuale.

   Per fare in modo che l'autenticazione vada a buon fine, l'amministratore deve disporre almeno dei seguenti diritti:

   - Diritto **Lettura** nell'area funzionale **Caratteristiche generali → Funzionalità di base**
   - Diritto **Lettura** nell'area funzionale **Caratteristiche generali → Administration Server virtuali**

L'applicazione salva i diritti utente modificati nell'account amministratore.

Configurazione dei diritti di accesso assegnando ruoli utente

In alternativa, è possibile concedere i diritti di accesso a un amministratore dell'Administration Server virtuale tramite i ruoli utente. Questo potrebbe ad esempio essere utile se si desidera assegnare più amministratori nello stesso Administration Server virtuale. In tal caso, è possibile assegnare agli account degli amministratori gli stessi ruoli utente (uno o più di questi) anziché configurare gli stessi diritti utente per più amministratori.

Per assegnare un amministratore a un Administration Server virtuale assegnando ruoli utente:

1. Nell'Administration Server primario creare un nuovo ruolo utente, quindi specificare tutti i diritti di accesso necessari di cui un amministratore deve disporre nell'Administration Server virtuale. È possibile creare più ruoli, ad esempio, se si desidera separare l'accesso a diverse aree funzionali.
2. Nella menu principale, passare all'Administration Server virtuale desiderato:
   a. Fare clic sull'icona a forma di freccia di espansione (›) a destra del nome corrente dell'Administration Server.
   b. Selezionare l'Administration Server desiderato.
3. Assegnare il nuovo ruolo o diversi ruoli all'account amministratore.

L'applicazione assegna i ruoli all'account amministratore.

Configurazione dei diritti di accesso a livello di oggetto

Oltre ad assegnare diritti di accesso a livello di area funzionale, è possibile configurare l'accesso a oggetti specifici nell'Administration Server virtuale, ad esempio, a un gruppo di amministrazione specifico o a un'attività. A tale scopo, passare all'Administration Server virtuale, quindi configurare i diritti di accesso nelle proprietà dell'oggetto.

Modifica di Administration Server per i dispositivi client

È possibile sostituire l'Administration Server che gestisce i dispositivi client con un altro server mediante l'attività *Cambia Administration Server*. Dopo il completamento dell'attività, i dispositivi client selezionati passeranno sotto la gestione dell'Administration Server specificato.

> Non è possibile utilizzare l'attività *Cambia Administration Server* per i dispositivi client connessi ad Administration Server tramite gateway di connessione. Per tali dispositivi è necessario riconfigurare Network Agent o reinstallarlo e specificare il gateway di connessione.

Per sostituire l'Administration Server che gestisce i dispositivi client con un altro server:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nel passaggio **Nuova attività**, specificare le seguenti impostazioni:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Security Center**.

   b. Nel campo **Tipo di attività**, selezionare **Cambia Administration Server**.

   c. Nel campo **Nome attività**, specificare il nome dell'attività che si intende creare.

      Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

   d. Selezionare i dispositivi a cui assegnare l'attività:

   - Assegna attività a un gruppo di amministrazione

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

     Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

   - Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco

     È possibile specificare nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

     Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

   - Assegna attività a una selezione dispositivi

     L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

4. Nel passaggio **Ambito attività** della procedura guidata, specificare un gruppo di amministrazione, dispositivi con indirizzi specifici o una selezione di dispositivi.

5. In questo passaggio della procedura guidata, confermare di accettare i termini di modifica di Administration Server per i dispositivi client.

6. In questo passaggio della procedura guidata, selezionare l'Administration Server che si desidera utilizzare per gestire i dispositivi selezionati:

   - Passa a un altro Administration Server primario

Per spostare i dispositivi client su un altro Administration Server primario, specificare le seguenti impostazioni di connessione dell'Administration Server:

1. Nel campo **Indirizzo di Administration Server**, specificare l'indirizzo del nuovo Administration Server primario.
2. Nel campo **Numero di porta**, specificare il numero di porta per connettersi all'Administration Server.

   Il numero di porta predefinito è 14000.
3. Nel campo **Porta SSL**, specificare il numero della porta SSL nell'Administration Server primario.

   Il numero di porta predefinito è 13000.
4. Se necessario, abilitare l'opzione **Usa server proxy**.

   Se questa opzione è disabilitata, viene utilizzata la connessione diretta per connettere il dispositivo all'Administration Server.

   Se questa opzione è abilitata, specificare i parametri del server proxy:

   - **Indirizzo server proxy**
   - **Porta server proxy**

   Se il server proxy richiede l'autenticazione, nei campi **Nome utente** e **Password** specificare le credenziali dell'account con cui viene stabilita la connessione al server proxy. È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.
5. Se necessario, caricare un nuovo certificato di Administration Server.

- Passa a un altro server virtuale in questo server primario

  Selezionare questa opzione per spostare i dispositivi client sull'Administration Server virtuale sull'Administration Server primario corrente. A tale scopo, nell'elenco a discesa **Nome Administration Server virtuale**, selezionare l'Administration Server virtuale necessario.

7. Nel passaggio **Selezione di un account per l'esecuzione dell'attività** della procedura guidata, specificare le impostazioni dell'account:

- Account predefinito

  L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

  Per impostazione predefinita, questa opzione è selezionata.

- Specifica account

  Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

  - Account

    Account tramite il quale viene eseguita l'attività.

- **Password**

  Password dell'account con cui verrà eseguita l'attività.

8. Se si desidera modificare le impostazioni predefinite dell'attività, nella fase **Completa creazione attività** della procedura guidata, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione**.

   Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

9. Fare clic sul pulsante **Fine**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.

10. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

11. Se si desidera modificare le impostazioni predefinite dell'attività, nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

12. Fare clic sul pulsante **Salva**.

    L'attività verrà creata e configurata.

13. Eseguire l'attività creata.

Dopo il completamento dell'attività, i dispositivi client per cui è stata creata passano sotto la gestione dell'Administration Server specificato nelle impostazioni dell'attività.

Eliminazione di un Administration Server virtuale

Quando si elimina un Administration Server virtuale, verranno eliminati anche tutti gli oggetti creati nell'Administration Server, inclusi criteri e attività. I dispositivi gestiti dei gruppi di amministrazione che erano gestiti dall'Administration Server virtuale verranno rimossi dai gruppi di amministrazione. Per far tornare i dispositivi sotto la gestione di Kaspersky Security Center Linux, eseguire il polling di rete, quindi spostare i dispositivi rilevati dal gruppo Dispositivi non assegnati ai gruppi di amministrazione.

Per eliminare un Administration Server virtuale:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome di Administration Server.

2. Nella pagina visualizzata passare alla scheda **Administration Server**.

3. Selezionare l'Administration Server virtuale che si desidera eliminare.

4. Nella riga del menu fare clic sul pulsante **Elimina**.

L'Administration Server virtuale viene eliminato.

Configurazione della registrazione degli eventi di connessione ad Administration Server

È possibile salvare in un file di registro la cronologia delle connessioni e dei tentativi di connessione all'Administration Server durante l'esecuzione. Le informazioni nel file consentono di tenere traccia non solo delle connessioni all'interno dell'infrastruttura di rete, ma anche dei tentativi non autorizzati di accesso al server.

Per registrare gli eventi di connessione all'Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Porte di connessione**.

3. Abilitare l'opzione **Registra eventi di connessione ad Administration Server**.

Tutti gli ulteriori eventi di connessione in entrata all'Administration Server, i risultati di autenticazione e gli errori SSL verranno salvati nel file /var/opt/kaspersky/klnagent_srv/logs/sc.syslog.

Impostazione del numero massimo di eventi nell'archivio eventi

Nella sezione **Archivio eventi** della finestra delle proprietà di Administration Server è possibile modificare le impostazioni per l'archiviazione degli eventi nel database di Administration Server, limitando il numero di record degli eventi e il periodo di archiviazione dei record. Quando si specifica il numero massimo di eventi, l'applicazione calcola approssimativamente la quantità di spazio di archiviazione necessario per il numero specificato. È possibile utilizzare questo calcolo approssimativo per valutare se è necessario liberare spazio su disco per evitare l'overflow del database. La capacità predefinita del database di Administration Server è di 400.000 eventi. La capacità massima consigliata del database è di 45 milioni di eventi.

L'applicazione controlla il database ogni 10 minuti. Se il numero di eventi raggiunge il valore massimo specificato più 10.000, l'applicazione elimina gli eventi meno recenti in modo che rimanga solo il numero massimo di eventi specificato.

Quando l'Administration Server elimina gli eventi meno recenti, non può salvare i nuovi eventi nel database. Durante questo periodo, le informazioni sugli eventi rifiutati vengono scritte nel registro del sistema operativo. I nuovi eventi vengono accodati e quindi salvati nel database al termine dell'operazione di eliminazione. Per impostazione predefinita, la coda degli eventi è limitata a 20.000 eventi. È possibile personalizzare il limite della coda modificando il valore del contrassegno KLEVP_MAX_POSTPONED_CNT.

Per limitare il numero di eventi che è possibile archiviare nell'archivio eventi di Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Archivio eventi**. Specificare il numero massimo di eventi archiviati nel database.

3. Fare clic sul pulsante **Salva**.

Inoltre, è possibile procedere come segue:

- Modificare le impostazioni di qualsiasi attività per salvare gli eventi relativi all'avanzamento dell'attività oppure salvare solo i risultati dell'esecuzione dell'attività.

- Ridurre o disabilitare il periodo di archiviazione per gli eventi delle applicazioni di Administration Server, Network Agent e Kaspersky installate nei dispositivi gestiti.

In tal modo si riduce il numero di eventi nel database, si aumenta la velocità di esecuzione degli scenari associati all'analisi della tabella degli eventi nel database e si limita il rischio che gli eventi critici vengano sovrascritti da un ampio numero di eventi.

Spostamento di Administration Server in un altro dispositivo

Se è necessario utilizzare Administration Server in un nuovo dispositivo, è possibile spostarlo in uno dei seguenti modi:

- Spostare Administration Server e il server di database in un nuovo dispositivo (il server di database può essere installato nel nuovo dispositivo insieme ad Administration Server o in un altro dispositivo).
- Mantenere il server di database nel dispositivo precedente e spostare solo Administration Server in un nuovo dispositivo.

Per spostare Administration Server e il server di database in un nuovo dispositivo:

1. Nel dispositivo precedente creare un backup dei dati di Administration Server.

   A tale scopo è possibile eseguire l'attività di backup dei dati tramite Kaspersky Security Center Web Console o eseguire l'utilità klbackup.

2. Nel dispositivo precedente, disconnettere Administration Server dalla rete.

3. Selezionare un nuovo dispositivo in cui installare Administration Server. Assicurarsi che l'hardware e il software nel dispositivo selezionato soddisfino i requisiti per Administration Server, Kaspersky Security Center Web Console e Network Agent. Controllare inoltre che le porte utilizzate in Administration Server siano disponibili.

4. Assegnare lo stesso indirizzo al nuovo dispositivo.

   È possibile assegnare al nuovo Administration Server il nome NetBIOS, l'FQDN e l'indirizzo IP statico. Dipende dall'indirizzo di Administration Server impostato nel pacchetto di installazione di Network Agent al momento della distribuzione dei Network Agent. In alternativa, è possibile utilizzare l'indirizzo di connessione che determina l'Administration Server a cui Network Agent si connette (è possibile ottenere questo indirizzo nei dispositivi gestiti utilizzando l'utilità klnagchk).

5. Se nececessario, in un altro dispositivo installare il sistema di gestione database (DBMS) che verrà utilizzato da Administration Server.

   Il database può essere installato nel nuovo dispositivo insieme ad Administration Server o in un altro dispositivo. Verificare che questo dispositivo soddisfi i requisiti hardware e software. Quando si seleziona un DBMS, tenere in considerazione il numero di dispositivi coperti da Administration Server.

6. Installare Administration Server nel nuovo dispositivo.

   Se si sposta il server del database in un altro dispositivo, specificare l'indirizzo locale come indirizzo IP del dispositivo in cui è installato il database (la voce "h" nell'istruzione Installazione di Kaspersky Security Center Linux). Se è necessario mantenere il server del database nel dispositivo precedente, inserire l'indirizzo IP del dispositivo precedente nella voce “h” dell'istruzione Installazione di Kaspersky Security Center Linux.

7. Al termine dell'installazione ripristinare i dati di Administration Server nel nuovo dispositivo utilizzando l'utilità klbackup.

8. Aprire Kaspersky Security Center Web Console e connettersi ad Administration Server.

9. Verificare che tutti i dispositivi gestiti vengano collegati ad Administration Server.

10. Disinstallare Administration Server e il server del database dal dispositivo precedente.

Modifica delle credenziali del DBMS

Talvolta potrebbe essere necessario modificare le credenziali del DBMS, ad esempio per eseguire una rotazione delle credenziali per motivi di sicurezza.

Per modificare le credenziali del DBMS in un ambiente Linux tramite l'utilità klsrvconfig:

1. Avviare una riga di comando di Linux.

2. Specificare l'utilità klsrvconfig nella finestra della riga di comando aperta:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klsrvconfig -set_dbms_cred
   ```

3. Specificare un nome per il nuovo account. È necessario specificare le credenziali di un account esistente nel DBMS.

4. Immettere una nuova password.

5. Specificare la nuova password per la conferma.

Le credenziali del DBMS vengono modificate.

Backup e ripristino dei dati di Administration Server

Il backup dei dati consente di spostare un Administration Server da un dispositivo all'altro senza perdite di dati. Tramite il backup, è possibile ripristinare i dati durante lo spostamento del database di Administration Server in un altro dispositivo o durante l'upgrade a una versione più recente di Kaspersky Security Center Linux (lo spostamento dei dati di Administration Server per la gestione di Kaspersky Security Center Windows non è supportato).

Non viene eseguito il backup dei plug-in di gestione installati. Dopo aver ripristinato i dati di Administration Server da una copia di backup, è necessario scaricare e reinstallare i plug-in per le applicazioni gestite.

Prima di eseguire il backup dei dati di Administration Server, verificare se al gruppo di amministrazione è stato aggiunto un Administration Server virtuale. Se viene aggiunto un Administration Server virtuale, assicurarsi che a questo Administration Server virtuale sia assegnato un amministratore prima del backup. Non è possibile concedere all'amministratore i diritti di accesso all'Administration Server virtuale dopo il backup. Tenere presente che se le credenziali dell'account amministratore vengono smarrite, non sarà possibile assegnare un nuovo amministratore all'Administration Server virtuale.

È possibile creare una copia di backup dei dati di Administration Server in uno dei seguenti modi:

- Creando ed eseguendo un'attività di backup dei dati tramite Kaspersky Security Center Web Console.

- Eseguendo l'utilità klbackup nel dispositivo in cui è installato Administration Server. Questa utilità è inclusa nel kit di distribuzione di Kaspersky Security Center. Dopo l'installazione di Administration Server, l'utilità è disponibile

nella radice della cartella di destinazione specificata durante l'installazione dell'applicazione (in genere, /opt/kaspersky/ksc64/sbin/klbackup).

I seguenti dati vengono salvati nella copia di backup di Administration Server:

- Database di Administration Server (criteri, attività, impostazioni delle applicazioni, eventi salvati in Administration Server).
- Dettagli sulla configurazione della struttura dei gruppi di amministrazione e dei dispositivi client.
- Archivio dei pacchetti di distribuzione delle applicazioni per l'installazione remota.
- Certificato di Administration Server.

Il ripristino dei dati di Administration Server è possibile solo tramite l'utilità klbackup.

Creazione di un'attività di backup dei dati di Administration Server

Le attività di backup sono attività di Administration Server, create tramite l'avvio rapido guidato. Se un'attività di backup creata dall'Avvio rapido guidato è stata eliminata, è possibile crearne una manualmente.

L'attività *Backup dei dati di Administration Server* può essere creata solo in una singola copia. Se l'attività di backup dei dati di Administration Server è stata già creata per l'Administration Server, non viene visualizzata nella finestra di selezione del tipo di attività.

Per creare un'attività di backup dei dati di Administration Server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Nell'elenco **Applicazione** selezionare **Kaspersky Security Center 15** e nell'elenco **Tipo di attività** selezionare **Backup dei dati di Administration Server**.
4. Nel passaggio corrispondente, specificare le seguenti informazioni:
   - Cartella per l'archiviazione delle copie di backup
   - Password per il backup (opzionale)
   - Numero massimo di copie di backup da salvare
5. Se nel passaggio **Completa creazione attività** si abilita l'opzione **Apri i dettagli dell'attività al termine della creazione**, è possibile modificare le impostazioni predefinite dell'attività. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
6. Fare clic sul pulsante **Fine**.

L'attività verrà creata e visualizzata nell'elenco delle attività.

Utilizzo dell'utilità klbackup per eseguire il backup e il ripristino dei dati

È possibile copiare i dati di Administration Server a scopo di backup e per il ripristino in un secondo momento tramite l'utilità klbackup, inclusa nel kit di distribuzione di Kaspersky Security Center.

L'istanza di Administration Server in cui deve essere eseguito il ripristino deve utilizzare un DBMS dello stesso tipo. La versione di Administration Server può essere la stessa (con una patch identica o successiva) o una versione successiva.

Se è stato eseguito il backup dei dati di Administration Server inclusi in Kaspersky Security Center Linux 15 o versione precedente quando si utilizza il DBMS MariaDB di una versione precedente e quindi si ripristinano i dati in un dispositivo con una versione successiva di MariaDB, è possibile che si verifichi un errore. Per ulteriori informazioni, fare riferimento a Come ripristinare i dati di Administration Server da un backup creato in una versione precedente del DBMS.

I flag di Network Agent non vengono ripristinati quando si utilizza l'utilità klbackup. È necessario configurare manualmente i flag di Network Agent.

Per creare una copia di backup o eseguire il ripristino dei dati di Administration Server in modalità automatica:

Eseguire klbackup con il set di chiavi desiderato dalla riga di comando del dispositivo in cui è installato Administration Server.

Sintassi della riga di comando per l'utilità:

```
klbackup -path BACKUP_PATH [-linux_path LINUX_PATH][-node_cert CERT_PATH] [-logfile
LOGFILE] [-use_ts]|[-restore] [-password PASSWORD]
```

Se non viene specificata alcuna password nella riga di comando dell'utilità klbackup, verrà richiesto di immetterla nella modalità interattiva.

Descrizioni delle chiavi:

- `-path BACKUP_PATH` — Salvare le informazioni nella cartella BACKUP_PATH o utilizzare i dati nella cartella BACKUP_PATH per il ripristino (parametro obbligatorio).
- `-linux_path LINUX_PATH` — Percorso locale della cartella con i dati di backup del DBMS.

  È necessario concedere all'account del server database e all'utilità klbackup le autorizzazioni per la modifica dei dati nella cartella LINUX_PATH.
- `-node_cert CERT_PATH` — file del certificato del server per configurare il nodo del cluster di failover inattivo dopo il ripristino. Se non è impostato, verrà recuperato automaticamente dal server.
- `-logfile LOGFILE` — Salvare un rapporto sul backup e il ripristino dei dati di Administration Server.

  È necessario concedere all'account del server database e all'utilità klbackup le autorizzazioni per la modifica dei dati nella cartella PERCORSO_BACKUP.

- `-use_ts` — Quando si salvano i dati, copiare le informazioni nella cartella BACKUP_PATH, nella sottocartella con un nome nel formato `klbackup YYYY-MM-DD # HH-MM-SS`, che include la data corrente e l'ora dell'operazione in UTC. Se la chiave non è specificata, le informazioni vengono salvate nella radice della cartella BACKUP_PATH.

  Quando si tenta di salvare le informazioni in una cartella in cui è già presente una copia di backup, viene visualizzato un messaggio di errore. Le informazioni non vengono aggiornate.

  La disponibilità della chiave `-use_ts` consente la gestione di un archivio dei dati di Administration Server. Ad esempio, se la chiave `-path` indica la cartella `/tmp/KLBackups`, nella cartella `klbackup 2022/6/19 # 11-30-18` vengono archiviate le informazioni sullo stato dell'Administration Server in data 19 giugno 2022 alle 11:30:18.

- `-restore` — Ripristinare i dati di Administration Server. Il ripristino dei dati viene eseguito in base alle informazioni contenute nella cartella BACKUP_PATH. Se non è disponibile nessuna chiave, viene eseguito il backup dei dati nella cartella BACKUP_PATH.

- `-password PASSWORD` — password per proteggere i dati sensibili.

  Non è possibile recuperare una password dimenticata. Non sono disponibili requisiti per la password. La lunghezza della password è illimitata ed è possibile anche la lunghezza zero (nessuna password).

  Al momento del ripristino dei dati, è necessario specificare la stessa password che è stata immessa durante il backup. Se il percorso di una cartella condivisa è stato modificato dopo il backup, controllare l'esecuzione delle attività che utilizzano i dati ripristinati (attività di ripristino e attività di installazione remota). Se necessario, modificare le impostazioni di queste attività. Durante il ripristino dei dati da un file di backup, nessun utente deve accedere alla cartella condivisa di Administration Server. L'account con cui viene avviata l'utilità klbackup deve avere accesso completo alla cartella condivisa. Per ripristinare i dati di Administration Server dal backup, è consigliabile eseguire l'utilità in un Administration Server appena installato.

Manutenzione di Administration Server

La manutenzione di Administration Server consente di liberare spazio nella cartella di Administration Server e ridurre il volume del database eliminando gli oggetti non più necessari. Ciò consente di migliorare le prestazioni e l'affidabilità operativa dell'applicazione. È consigliabile eseguire la manutenzione di Administration Server almeno ogni settimana.

La manutenzione di Administration Server viene eseguita tramite un'attività specializzata. Durante la manutenzione di Administration Server, l'applicazione esegue le azioni seguenti:

- Elimina le cartelle e i file non necessari dalla cartella di archiviazione.
- Elimina i record non necessari dalle tabelle (noti anche come "puntatori pendenti").
- Cancella la cache.
- Esegue la manutenzione del database (se si utilizza PostgreSQL come DBMS):
  - Riorganizza gli indici del database.
  - Aggiorna le statistiche del database.
  - Riduce le dimensioni del database (se necessario).

L'attività Manutenzione di Administration Server supporta le versioni MariaDB 10.3 e successive. Se si utilizza MariaDB 10.2 o versioni precedenti, gli amministratori devono mantenere questo DBMS in autonomia.

L'attività di Manutenzione di Administration Server viene creata automaticamente durante l'installazione di Kaspersky Security Center Linux. Se l'attività di Manutenzione di Administration Server viene eliminata, è possibile crearla manualmente.

Per creare l'attività di Manutenzione di Administration Server:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.
3. Nella finestra **Nuova attività** della procedura guidata selezionare **Manutenzione di Administration Server** come tipo di attività e fare clic su **Avanti**.
4. Seguire le rimanenti istruzioni della procedura guidata.

La nuova attività creata verrà visualizzata nell'elenco delle attività. Una sola attività di Manutenzione di Administration Server può essere in esecuzione per un singolo Administration Server. Se è stata già creata l'attività di Manutenzione di Administration Server per un Administration Server, non può essere creata alcuna nuova attività di Manutenzione di Administration Server.

Eliminazione di una gerarchia di Administration Server

Se non si desidera più avere una gerarchia di Administration Server, è possibile disconnetterli da tale gerarchia.

Per eliminare una gerarchia di Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server primario.
2. Nella pagina visualizzata passare alla scheda **Administration Server**.
3. Nel gruppo di amministrazione da cui si desidera eliminare l'Administration Server secondario selezionare l'Administration Server secondario.
4. Nella riga del menu fare clic su **Elimina**.
5. Nella finestra di dialogo visualizzata fare clic su **OK** per confermare che si desidera eliminare l'Administration Server secondario.

   I precedenti Administration Server primario e secondario sono ora indipendenti l'uno dall'altro. La gerarchia non è più presente.

Accesso ai server DNS pubblici

Se non è possibile accedere ai server Kaspersky utilizzando il DNS di sistema, Kaspersky Security Center Linux può utilizzare i seguenti server DNS pubblici, nel seguente ordine:

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)

Le richieste a questi server DNS possono contenere indirizzi di dominio e l'indirizzo IP pubblico di Administration Server, poiché l'applicazione stabilisce una connessione TCP/UDP al server DNS. Se Kaspersky Security Center Linux utilizza un server DNS pubblico, il trattamento dei dati è disciplinato dall'informativa sulla privacy del servizio pertinente.

Per configurare l'uso del DNS pubblico tramite l'utilità klscflag:

1. Eseguire la riga dei comandi, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella directory in cui è installato Administration Server. Il percorso di installazione predefinito è /opt/kaspersky/ksc64/sbin.

2. Per disabilitare l'uso del DNS pubblico, eseguire il seguente comando nell'account root:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Per abilitare l'uso del DNS pubblico, eseguire il seguente comando nell'account root:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Configurazione dell'interfaccia

È possibile configurare l'interfaccia di Kaspersky Security Center Web Console in modo da visualizzare e nascondere sezioni ed elementi di interfaccia, a seconda delle funzionalità utilizzate.

Per configurare l'interfaccia di Kaspersky Security Center Web Console in base al set di funzionalità utilizzate al momento:

1. Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Opzioni di interfaccia**.

2. Nella finestra **Opzioni di interfaccia** visualizzata abilitare o disabilitare l'opzione **Mostra Criptaggio e protezione dei dati**.

3. Fare clic su **Salva**.

   Successivamente, nel menu principale viene visualizzata la sezione **Operazioni → Criptaggio e protezione dei dati**.

Criptaggio delle comunicazioni con TLS

Per correggere le vulnerabilità nella rete aziendale dell'organizzazione, è possibile abilitare il criptaggio del traffico tramite il protocollo TLS. È possibile abilitare i protocolli di criptaggio TLS e i pacchetti di criptaggio supportati in Administration Server. Kaspersky Security Center Linux supporta le versioni del protocollo TLS 1.0, 1.1, 1.2 e 1.3. È possibile selezionare il protocollo e i pacchetti di criptaggio richiesti.

Kaspersky Security Center Linux utilizza certificati autofirmati. È inoltre possibile utilizzare i propri certificati. Gli specialisti di Kaspersky consigliano di utilizzare i certificati rilasciati da autorità di certificazione attendibili.

Per configurare i protocolli e i pacchetti di criptaggio consentiti in Administration Server:

1. Eseguire la riga dei comandi, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella directory in cui è installato Administration Server. Il percorso di installazione predefinito è /opt/kaspersky/ksc64/sbin.

2. Utilizzare il contrassegno SrvUseStrictSslSettings per configurare i protocolli e i pacchetti di criptaggio consentiti in Administration Server. Eseguire il seguente comando nella riga di comando nell'account root:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <valore> -t d
   ```

   Specificare il parametro <valore> del contrassegno SrvUseStrictSslSettings:

   - 4: Sono abilitati solo i protocolli TLS 1.2 e TLS 1.3. Sono abilitate anche le suite di criptaggio con TLS_RSA_WITH_AES_256_GCM_SHA384 (queste suite di criptaggio sono necessarie per la retrocompatibilità con le versioni precedenti di Kaspersky Security Center Linux). Questo è il valore predefinito.

     Suite di criptaggio supportate per il protocollo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (suite di criptaggio con TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Suite di criptaggio supportate per il protocollo TLS 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - 5: Sono abilitati solo i protocolli TLS 1.2 e TLS 1.3. Per i protocolli TLS 1.2 e TLS 1.3, sono supportati i pacchetti di criptaggio specifici elencati di seguito.

     Suite di criptaggio supportate per il protocollo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Suite di criptaggio supportate per il protocollo TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Non è consigliabile utilizzare 0, 1, 2 o 3 come valore del parametro del contrassegno SrvUseStrictSslSettings. Questi valori dei parametri corrispondono a versioni non sicure del protocollo TLS (TLS 1.0 e TLS 1.1) e a suite di criptaggio non sicure e vengono utilizzati solo per la compatibilità con le versioni precedenti di Kaspersky Security Center.

3. Riavviare i seguenti servizi Kaspersky Security Center Linux:
   - Administration Server
   - Server Web
   - Proxy di attivazione

Di conseguenza, il criptaggio del traffico utilizzando il protocollo TLS è abilitato.

È possibile utilizzare i contrassegni KLTR_TLS12_ENABLED e KLTR_TLS13_ENABLED per abilitare rispettivamente il supporto dei protocolli TLS 1.2 e TLS 1.3. Questi contrassegni sono abilitati per impostazione predefinita.

Per abilitare o disabilitare il supporto dei protocolli TLS 1.2 e TLS 1.3:

1. Eseguire l'utilità klscflag.

   Eseguire la riga dei comandi, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella directory in cui è installato Administration Server. Il percorso di installazione predefinito è /opt/kaspersky/ksc64/sbin.

2. Eseguire uno dei seguenti comandi nella riga di comando nell'account root:
   - Utilizzare questo comando per abilitare o disabilitare il supporto del protocollo TLS 1.2:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <valore> -t d
     ```

   - Utilizzare questo comando per abilitare o disabilitare il supporto del protocollo TLS 1.3:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <valore> -t d
     ```

   Specificare il parametro <valore> del contrassegno:
   - `1`: Per abilitare il supporto del protocollo TLS.
   - `0`: Per disabilitare il supporto del protocollo TLS.

Elenco globale delle subnet

Per ogni Administration Server in uso, è possibile impostare un elenco globale delle subnet in cui archiviare le informazioni sulle subnet della rete. Questo elenco consente di associare coppie {indirizzo IP, maschera} e unità fisiche, come ad esempio le filiali. È possibile utilizzare le subnet in questo elenco nelle regole e nelle impostazioni di rete.

Per aggiungere una subnet all'elenco globale delle subnet:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale**, selezionare la sezione **Subnet globali**.

3. Fare clic sul pulsante **Aggiungi**.

   Verrà aperta la finestra **Nuova subnet**.

4. Compilare i seguenti campi:

   - **Nome**
   - **Indirizzo subnet**
   - **Subnet mask**
   - **Descrizione**

5. Fare clic sul pulsante **Salva**.

La finestra viene chiusa e la subnet viene visualizzata nell'elenco delle subnet.

Se necessario, nell'elenco delle subnet globali è possibile eseguire le seguenti operazioni:

- Eliminare le subnet dall'elenco selezionando la subnet richiesta e facendo clic sul pulsante **Rimuovi**.
- Modificare le proprietà delle subnet facendo clic sul collegamento con il nome della subnet richiesta, quindi eseguendo le azioni descritte nei passaggi 4–5.

Individuazione dei dispositivi nella rete

Questa sezione descrive la ricerca e l'individuazione dei dispositivi nella rete.

Kaspersky Security Center Linux consente di individuare i dispositivi sulla base dei criteri specificati. È possibile salvare i risultati della ricerca in un file di testo.

La funzionalità di ricerca e individuazione consente di trovare i seguenti dispositivi:

- I dispositivi gestiti nei gruppi di amministrazione di Kaspersky Security Center Administration Server e nei relativi Administration Server secondari.
- I dispositivi non assegnati gestiti da Kaspersky Security Center Administration Server e dai relativi Administration Server secondari.

Scenario: Individuazione dei dispositivi nella rete

È necessario eseguire la device discovery prima dell'installazione delle applicazioni di protezione. Quando vengono individuati tutti i dispositivi della rete, è possibile ricevere informazioni in merito e gestirli tramite i criteri. Il polling periodico della rete è necessario per scoprire se sono presenti nuovi dispositivi e se i dispositivi individuati in precedenza sono ancora in rete.

L'individuazione dei dispositivi della rete comprende le seguenti fasi:

1. **Device discovery iniziale**

   Dopo aver completato l'avvio rapido guidato, eseguire manualmente la device discovery.

2. **Configurazione delle operazioni di polling future**

   Verificare che il polling dell'intervallo IP sia abilitato e che la pianificazione di polling soddisfi le esigenze dell'organizzazione. Durante la configurazione la pianificazione di polling utilizzare i suggerimenti per la frequenza di polling della rete.

   È inoltre possibile abilitare Polling Zeroconf se la rete include dispositivi IPv6.

   Se i dispositivi in rete sono inclusi in un dominio, è consigliabile utilizzare il polling del controller di dominio.

3. **Configurazione delle regole per l'aggiunta dei dispositivi individuati nei gruppi di amministrazione (opzione facoltativa)**

   Se vengono visualizzati nuovi dispositivi nella rete, questi vengono individuati durante il polling periodico e vengono automaticamente inclusi nel gruppo **Dispositivi non assegnati**. Se si desidera, è possibile configurare le regole per lo spostamento automatico di questi dispositivi nel gruppo **Dispositivi gestiti**. È inoltre possibile definire le regole di conservazione.

   Se si ignora questa fase di configurazione delle regole, tutti i nuovi dispositivi individuati passano al gruppo **Dispositivi non assegnati** e rimangono in tale gruppo. Se si desidera, è possibile spostare questi dispositivi nel gruppo **Dispositivi gestiti** manualmente. Se si spostano manualmente i dispositivi nel gruppo **Dispositivi gestiti**, è possibile analizzare le informazioni su ciascun dispositivo, decidere se spostarlo in un gruppo di amministrazione e, in tal caso, in quale gruppo.

Risultati

Il completamento dello scenario dà i seguenti risultati:

- Kaspersky Security Center Linux Administration Server rileva i dispositivi nella rete e fornisce informazioni in merito.
- Le operazioni di polling future vengono impostate ed eseguite in base alla pianificazione specificata.

I nuovi dispositivi individuati vengono organizzati in base alle regole configurate. In alternativa, se non è configurata alcuna regola, i dispositivi rimangono nel gruppo **Dispositivi non assegnati**).

Polling intervallo IP

Kaspersky Security Center Linux tenta di eseguire la risoluzione inversa dei nomi per ogni indirizzo IPv4 nell'intervallo specificato a un nome DNS utilizzando richieste DNS standard. Se questa operazione riesce, il server invia un messaggio `ICMP ECHO REQUEST` (equivalente al comando ping) al nome ricevuto. Se il dispositivo risponde, le informazioni su di esso vengono aggiunte al database di Kaspersky Security Center Linux. La risoluzione inversa dei nomi è necessaria per escludere i dispositivi di rete che possono avere un indirizzo IP ma che non sono computer, ad esempio stampanti o router di rete.

Questo metodo di polling si basa su un servizio DNS locale configurato correttamente. Deve essere presente una zona di ricerca inversa. Se questa zona non è configurata, il polling della subnet IP non produrrà risultati.

Inizialmente, Kaspersky Security Center Linux ottiene gli intervalli IP per il polling dalle impostazioni di rete del dispositivo in cui è installato. Se l'indirizzo del dispositivo è 192.168.0.1 e la subnet mask è 255.255.255.0, Kaspersky Security Center Linux include automaticamente la rete 192.168.0.0/24 nell'elenco degli indirizzi di polling. Kaspersky Security Center Linux esegue il polling di tutti gli indirizzi da 192.168.0.1 a 192.168.0.254.

Se è abilitato solo il polling dell'intervallo IP, Kaspersky Security Center Linux rileva i dispositivi solo con indirizzi IPv4. Se la rete include dispositivi IPv6, attivare la funzionalità Polling Zeroconf dei dispositivi.

Visualizzazione e modifica delle impostazioni per il polling degli intervalli IP

Per visualizzare e modificare le proprietà per il polling degli intervalli IP:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Intervalli IP**.
2. Fare clic sul pulsante **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del polling IP.
3. Abilitare o disabilitare il polling IP utilizzando l'interruttore **Consenti polling**.
4. Configurare la pianificazione del polling. Per impostazione predefinita, il polling IP viene eseguito ogni 420 minuti (sette ore).

   Quando si specifica l'intervallo di polling, verificare che questa impostazione non superi il valore del parametro di durata dell'indirizzo IP. Se un indirizzo IP non viene verificato tramite il polling durante la durata dell'indirizzo IP, tale indirizzo IP viene automaticamente rimosso dai risultati del polling. Per impostazione predefinita, la durata dei risultati del polling è di 24 ore, poiché gli indirizzi IP dinamici, ovvero assegnati tramite il protocollo DHCP (Dynamic Host Configuration Protocol), cambiano ogni 24 ore.

   Opzioni per la pianificazione di polling:

   - **Ogni N giorni**

Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N minuti**

  Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

- **In base ai giorni della settimana**

  Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

- **Esegui attività non effettuate**

  Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

  Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

  Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

  Per impostazione predefinita, questa opzione è disabilitata.

5. Fare clic sul pulsante **Salva**.

Le proprietà verranno salvate e applicate a tutti gli intervalli IP.

Esecuzione manuale del polling

Per eseguire immediatamente il polling:

Fare clic su **Avvia polling**.

Aggiunta e modifica di un intervallo IP

Inizialmente, Kaspersky Security Center Linux ottiene gli intervalli IP per il polling dalle impostazioni di rete del dispositivo in cui è installato. Se l'indirizzo del dispositivo è 192.168.0.1 e la subnet mask è 255.255.255.0, Kaspersky Security Center Linux include automaticamente la rete 192.168.0.0/24 nell'elenco degli indirizzi di polling. Kaspersky Security Center Linux esegue il polling di tutti gli indirizzi da 192.168.0.1 a 192.168.0.254. È possibile modificare gli intervalli IP definiti automaticamente o aggiungere intervalli IP personalizzati.

È possibile creare un intervallo solo per gli indirizzi IPv4. Se si abilita Polling Zeroconf, Kaspersky Security Center Linux eseguirà il polling dell'intera rete.

Per aggiungere un nuovo intervallo IP:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Intervalli IP**.
2. Per aggiungere un nuovo intervallo IP, fare clic sul pulsante **Aggiungi**.
3. Nella finestra visualizzata specificare le seguenti impostazioni:
   - **Nome intervallo IP**

     Nome dell'intervallo IP. È possibile specificare l'intervallo IP stesso come nome, ad esempio "192.168.0.0/24".

   - **Intervallo IP o indirizzo subnet e subnet mask**

     Impostare l'intervallo IP specificando gli indirizzi IP iniziale e finale o l'indirizzo subnet e la subnet mask. È inoltre possibile selezionare uno degli intervalli IP già esistenti facendo clic sul pulsante **Sfoglia**.

   - **Durata dell'indirizzo IP (ore)**

     Quando si specifica questo parametro, assicurarsi che superi l'intervallo di polling impostato nella pianificazione del polling. Se un indirizzo IP non viene verificato tramite il polling durante la durata dell'indirizzo IP, tale indirizzo IP viene automaticamente rimosso dai risultati del polling. Per impostazione predefinita, la durata dei risultati del polling è di 24 ore, poiché gli indirizzi IP dinamici, ovvero assegnati tramite il protocollo DHCP (Dynamic Host Configuration Protocol), cambiano ogni 24 ore.
4. Selezionare **Abilita polling intervalli IP** se si desidera eseguire il polling della subnet o dell'intervallo aggiunto. In caso contrario, non verrà effettuato il polling della subnet o dell'intervallo aggiunto.
5. Fare clic sul pulsante **Salva**.

Il nuovo intervallo IP verrà aggiunto all'elenco degli intervalli IP.

È possibile eseguire il polling di ciascun intervallo IP separatamente utilizzando il pulsante **Avvia polling**. Per impostazione predefinita, la durata dei risultati del polling è di 24 ore ed è uguale all'impostazione per la durata dell'indirizzo IP.

Per aggiungere una subnet a un intervallo IP esistente:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Intervalli IP**.
2. Fare clic sul nome dell'intervallo IP a cui si desidera aggiungere una subnet.
3. Nella finestra visualizzata fare clic sul pulsante **Aggiungi**.
4. Specificare una subnet utilizzando il relativo indirizzo e la subnet mask oppure tramite il primo e l'ultimo indirizzo IP nell'intervallo IP. In alternativa, aggiungere una subnet esistente facendo clic sul pulsante **Sfoglia**.
5. Fare clic sul pulsante **Salva**.

La nuova subnet verrà aggiunta all'intervallo IP.

6. Fare clic sul pulsante **Salva**.

Le nuove impostazioni dell'intervallo IP verranno salvate.

È possibile aggiungere tutte le subnet necessarie. Gli intervalli IP denominati non possono sovrapporsi, ma le subnet non denominate all'interno di un intervallo IP non presentano tali restrizioni. È possibile abilitare e disabilitare il polling in modo indipendente per ogni intervallo IP.

Polling zeroconf

Questo tipo di polling è supportato solo per i punti di distribuzione basati su Linux.

Kaspersky Security Center Linux può eseguire il polling delle reti che hanno dispositivi con indirizzi IPv6. In questo caso, gli intervalli IP non vengono specificati e Kaspersky Security Center Linux esegue il polling dell'intera rete utilizzando le reti zero-configuration (definite anche *Zeroconf*). Per iniziare a utilizzare Zeroconf, è necessario installare l'utilità avahi-browse nel dispositivo Linux che esegue il polling delle reti: un Administration Server o un punto di distribuzione.

Per abilitare il polling Zeroconf:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Intervalli IP**.
2. Fare clic sul pulsante **Proprietà**.
3. Nella finestra aperta, attivare l'interruttore **Usa Zeroconf per il polling delle reti IPv6**.

Successivamente, Kaspersky Security Center Linux inizia a eseguire il polling della rete. In questo caso gli intervalli IP specificati vengono ignorati.

Polling del controller di dominio

Kaspersky Security Center Linux supporta il polling di un controller di dominio Microsoft Active Directory e di un controller di dominio Samba. Per un controller di dominio Samba, Samba 4 viene utilizzato come controller di dominio Active Directory.

Quando si esegue il polling di un controller di dominio, Administration Server o un punto di distribuzione recuperano le informazioni sulla struttura del dominio, sugli account utente, sui gruppi di protezione e sui nomi DNS dei dispositivi inclusi nel dominio.

È consigliabile utilizzare il polling del controller di dominio se tutti i dispositivi in rete sono membri di un dominio. Se alcuni dei dispositivi in rete non sono inclusi nel dominio, questi dispositivi non possono essere rilevati dal polling del controller di dominio.

Il server invia richieste echo ICMP (uguali al comando ping) durante il polling di Microsoft Active Directory.

Prerequisiti

Prima di eseguire il polling di un controller di dominio, assicurarsi di consentire le connessioni al controller di dominio tramite un firewall o un server proxy. Verificare inoltre che i seguenti protocolli siano abilitati nel controller di dominio:

- Lightweight Directory Access Protocol (LDAP)
- Simple Authentication and Security Layer (SASL)

  Questo protocollo viene utilizzato se la connessione al controller di dominio viene stabilita utilizzando l'autenticazione SASL. Administration Server e i punti di distribuzione supportano solo il meccanismo DIGEST-MD5.
- Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS)

  Questo protocollo viene utilizzato se è necessario connettersi al controller di dominio tramite una connessione criptata.

Verificare che le seguenti porte siano disponibili nel dispositivo del controller di dominio:

- 389 per il protocollo LDAP e Simple Authentication (incluso SASL)
- 636 per il protocollo LDAPS

Polling del controller di dominio tramite Administration Server

Per eseguire il polling di un controller di dominio utilizzando Administration Server:

1. Nel menu principale, passare a **Individuazione e distribuzione** → **Individuazione** → **Controller di dominio**.
2. Fare clic su **Impostazioni di polling**.

   Viene visualizzata la finestra **Impostazioni di polling del controller di dominio**.
3. Selezionare l'opzione **Abilita polling controller di dominio**.
4. In **Esegui polling di domini specifici**, fare clic su **Aggiungi**, quindi specificare l'indirizzo e le credenziali utente del controller di dominio.
5. Se necessario, nella finestra **Impostazioni di polling del controller di dominio**, specificare la pianificazione del polling. Il periodo predefinito è un'ora. I dati ricevuti al successivo polling sostituiscono completamente i dati precedenti.

   Sono disponibili le opzioni di pianificazione di polling seguenti:

   - **Ogni N giorni**

     Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

     Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.
   - **Ogni N minuti**

     Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

- **In base ai giorni della settimana**

  Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

- **Esegui attività non effettuate**

  Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

  Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

  Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

  Per impostazione predefinita, questa opzione è disabilitata.

Se si modificano gli account utente in un gruppo di protezione del dominio, queste modifiche verranno visualizzate in Kaspersky Security Center Linux un'ora dopo il polling del controller di dominio.

6. Fare clic su **Salva** per applicare le modifiche.
7. Se si desidera eseguire immediatamente il polling, fare clic sul pulsante **Avvia polling**.

Polling del controller di dominio utilizzando un punto di distribuzione

È inoltre possibile eseguire il polling di un controller di dominio utilizzando un punto di distribuzione. Un dispositivo gestito basato su Windows o Linux può fungere da punto di distribuzione.

Per un punto di distribuzione Linux, sono supportati il polling di un controller di dominio Microsoft Active Directory e di un controller di dominio Samba.
Per un punto di distribuzione Windows, è supportato solo il polling di un controller di dominio Microsoft Active Directory.
Il polling con un punto di distribuzione Mac non è supportato.

Per configurare il polling del controller di dominio utilizzando il punto di distribuzione:

1. Aprire le proprietà del punto di distribuzione.
2. Selezionare la sezione **Polling del controller di dominio**.
3. Selezionare l'opzione **Abilita polling controller di dominio**.
4. Selezionare il controller di dominio di cui si desidera eseguire il polling.

   Se si utilizza un punto di distribuzione Linux, nella sezione **Esegui polling di domini specifici**, fare clic su **Aggiungi**, quindi specificare l'indirizzo e le credenziali utente del controller di dominio.

   Se si utilizza un punto di distribuzione Windows, è possibile selezionare una delle seguenti opzioni:

- **Esegui polling dominio corrente**
- **Esegui polling di tutta la foresta di dominio**
- **Esegui polling di domini specifici**

5. Fare clic sul pulsante **Imposta pianificazione di polling** per specificare le opzioni di pianificazione del polling, se necessario.

   Il polling viene avviato solo in base alla pianificazione specificata. L'avvio manuale del polling non è disponibile.

Al termine del polling, la struttura del dominio verrà visualizzata nella sezione **Controller di dominio**.

Se sono installate e attivate le regole di spostamento dei dispositivi, i nuovi dispositivi individuati vengono automaticamente inclusi nel gruppo **Dispositivi gestiti**. Se non sono state abilitate regole di spostamento, i nuovi dispositivi individuati vengono automaticamente inclusi nel gruppo **Dispositivi non assegnati**.

Gli account utente rilevati possono essere utilizzati per l'autenticazione del dominio in Kaspersky Security Center Web Console.

Autenticazione e connessione a un controller di dominio

Autenticazione e connessione a un controller di dominio durante il polling di un dominio

Durante il polling di un controller di dominio, Administration Server o un punto di distribuzione identifica il protocollo di connessione per stabilire la connessione iniziale al controller di dominio. Questo protocollo viene utilizzato per tutte le connessioni future al controller di dominio. Quando si stabilisce la connessione iniziale al controller di dominio, è possibile modificare le opzioni di connessione utilizzando il flag Network Agent (`KLNAG_LDAP_TLS_REQCERT` e `KLNAG_LDAP_SSL_CACERT`). È possibile configurare i flag Network Agent utilizzando klscflag come descritto in questo articolo.

La connessione iniziale a un controller di dominio procede come segue:

1. Administration Server o un punto di distribuzione tenta di connettersi al controller di dominio tramite LDAPS.

   Per impostazione predefinita, la verifica del certificato non è richiesta. Impostare il contrassegno `KLNAG_LDAP_TLS_REQCERT` su 1 per applicare la verifica del certificato.

   Possibili valori del contrassegno `KLNAG_LDAP_TLS_REQCERT`:

   - `0`: il certificato viene richiesto, ma se non viene fornito o se la verifica del certificato non è riuscita, la connessione TLS viene considerata ancora creata correttamente (valore predefinito).
   - `1`: è richiesta una verifica rigorosa del certificato del server LDAP.

   Per impostazione predefinita, quando il flag `KLNAG_LDAP_SSL_CACERT` non è specificato, per accedere alla catena di certificati viene utilizzato il percorso dipendente dal sistema operativo dell'autorità di certificazione (CA). Utilizzare il contrassegno `KLNAG_LDAP_SSL_CACERT` per specificare un percorso personalizzato.

2. Se la connessione LDAPS non riesce, Administration Server o un punto di distribuzione tenta di connettersi al controller di dominio tramite una connessione TCP non criptata tramite SASL (DIGEST-MD5).

Autenticazione e connessione a un controller di dominio durante l'autenticazione di un utente di dominio ad Administration Server

Quando un utente di dominio si autentica in Administration Server, Administration Server identifica il protocollo per stabilire la connessione al controller di dominio.

La connessione a un controller di dominio procede come segue:

1. Administration Server tenta di connettersi al controller di dominio tramite LDAPS.

   È richiesta una verifica rigorosa del certificato del server LDAP.

   Per impostazione predefinita, quando il flag `KLNAG_LDAP_SSL_CACERT` non è specificato, per accedere alla catena di certificati viene utilizzato il percorso dipendente dal sistema operativo dell'autorità di certificazione (CA). Utilizzare il contrassegno `KLNAG_LDAP_SSL_CACERT` per specificare un percorso personalizzato.

2. Se la connessione LDAPS non riesce, si verifica un errore di connessione al controller di dominio e gli altri protocolli di connessione non vengono utilizzati.

Configurazione dei contrassegni

È possibile utilizzare l'utilità klscflag per configurare i contrassegni.

Eseguire la riga dei comandi, quindi modificare la directory corrente nella directory con l'utilità klscflag. Nel dispositivo Administration Server, l'utilità klscflag si trova nella directory di installazione. Il percorso di installazione predefinito è /opt/kaspersky/ksc64/sbin.

Ad esempio, il seguente comando impone la verifica del certificato:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Configurazione di un controller di dominio Samba

Kaspersky Security Center Linux supporta un controller di dominio Linux in esecuzione solo su Samba 4.

Un controller di dominio Samba supporta le stesse estensioni dello schema di un controller di dominio Microsoft Active Directory. È possibile abilitare la piena compatibilità di un controller di dominio Samba con un controller di dominio Microsoft Active Directory utilizzando l'estensione dello schema Samba 4. Questa è un'azione facoltativa.

Si consiglia di abilitare la piena compatibilità di un controller di dominio Samba con un controller di dominio Microsoft Active Directory. In questo modo, si assicurerà la corretta interazione tra Kaspersky Security Center Linux e il controller di dominio Samba.

Per abilitare la piena compatibilità di un controller di dominio Samba con un controller di dominio Microsoft Active Directory:

1. Eseguire il seguente comando per utilizzare l'estensione dello schema RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Abilitare l'aggiornamento dello schema in un controller di dominio Samba. A tale scopo, aggiungere la seguente riga al file `/etc/samba/smb.conf`:

   ```
   dsdb:schema update allowed = true
   ```

Se l'aggiornamento dello schema viene completato con un errore, è necessario eseguire un ripristino completo del controller di dominio che funge da master dello schema.

Se si desidera eseguire correttamente il polling di un controller di dominio Samba, è necessario specificare il `netbios name` e i parametri del `workgroup` nel file `/etc/samba/smb.conf`.

Utilizzo della modalità dinamica VDI nei dispositivi client

Un'infrastruttura virtuale può essere distribuita in una rete aziendale utilizzando macchine virtuali temporanee. Kaspersky Security Center Linux è in grado di rilevare le macchine virtuali temporanee aggiungendo le relative informazioni al database di Administration Server. Dopo che un utente ha finito di utilizzare una macchina virtuale temporanea, quest'ultima viene rimossa dall'infrastruttura virtuale. Tuttavia, è possibile che un record relativo alla macchina virtuale rimossa venga salvato nel database di Administration Server. Inoltre, le macchine virtuali inesistenti possono essere visualizzate in Kaspersky Security Center Web Console.

Per evitare che le informazioni relative alle macchine virtuali non esistenti vengano salvate, Kaspersky Security Center Linux supporta la modalità dinamica per Virtual Desktop Infrastructure (VDI). L'amministratore può abilitare il supporto della modalità dinamica per VDI nelle proprietà del pacchetto di installazione di Network Agent da installare nella macchina virtuale temporanea.

Quando una macchina virtuale temporanea viene disabilitata, Network Agent notifica ad Administration Server che la macchina è stata disabilitata. Se la macchina virtuale è stata disabilitata correttamente, viene rimossa dall'elenco dei dispositivi connessi ad Administration Server. Se durante la disabilitazione della macchina virtuale si verificano errori e Network Agent non invia una notifica relativa alla macchina virtuale disabilitata ad Administration Server, verrà utilizzato uno scenario di backup. In questo scenario, una macchina virtuale viene rimossa dall'elenco dei dispositivi connessi ad Administration Server dopo tre tentativi non riusciti di sincronizzazione con Administration Server.

Abilitazione della modalità dinamica VDI nelle proprietà di un pacchetto di installazione per Network Agent

Per abilitare la modalità dinamica VDI:

1. Nel menu principale accedere a **Individuazione e distribuzione → Distribuzione e assegnazione → Pacchetti di installazione**.
2. Nel menu di scelta rapida del pacchetto di installazione di Network Agent selezionare **Proprietà**.

   Verrà visualizzata la finestra **Proprietà**.
3. Nella finestra **Proprietà**, selezionare la sezione **Avanzate**.
4. Nella sezione **Avanzate** selezionare l'opzione **Abilita modalità dinamica per VDI**.

Il dispositivo in cui deve essere installato Network Agent diventa parte di VDI.

Spostamento dei dispositivi da VDI a un gruppo di amministrazione

Per spostare i dispositivi inclusi in VDI in un gruppo di amministrazione:

1. Passare a **Risorse (dispositivi)** → **Regole di spostamento**.
2. Fare clic su **Aggiungi**.
3. Nella scheda **Condizioni delle regole**, selezionare la scheda **Macchine virtuali**.
4. Impostare la regola **Questa è una macchina virtuale** su **Sì** e **Parte di Virtual Desktop Infrastructure** su **Sì.**
5. Fare clic su **Salva**.

Best practice per la distribuzione

Kaspersky Security Center Linux è un'applicazione distribuita. Kaspersky Security Center Linux include le seguenti applicazioni:

- Administration Server - Il componente principale, progettato per la gestione dei dispositivi di un'organizzazione e l'archiviazione dei dati in un sistema DBMS.
- Kaspersky Security Center Web Console: lo strumento di base per l'amministratore. È possibile installare Kaspersky Security Center Web Console nello stesso dispositivo in cui è installato Administration Server o in un altro dispositivo.
- Network Agent – Utilizzato per gestire l'applicazione di protezione installata in un dispositivo, nonché per ottenere informazioni sul dispositivo e per trasferire queste informazioni ad Administration Server. I Network Agent vengono installati nei dispositivi di un'organizzazione.

La distribuzione di Kaspersky Security Center Linux nella rete di un'organizzazione viene eseguita come segue:

- Installazione di Administration Server
- Installazione di Kaspersky Security Center Web Console nel dispositivo dell'amministratore
- Installazione di Network Agent e dell'applicazione di protezione nei dispositivi dell'organizzazione

Guida all'hardening

Kaspersky Security Center Linux è progettato per l'esecuzione centralizzata delle attività di base di amministrazione e manutenzione nella rete di un'organizzazione. L'applicazione fornisce all'amministratore l'accesso a informazioni dettagliate sul livello di sicurezza della rete dell'organizzazione. Kaspersky Security Center Linux consente di configurare tutti i componenti della protezione creati utilizzando le applicazioni Kaspersky.

Kaspersky Security Center Linux Administration Server ha accesso completo alla gestione della protezione dei dispositivi client ed è il componente più importante del sistema di sicurezza dell'organizzazione. Pertanto, per Administration Server sono necessari metodi di protezione avanzati.

Prima della configurazione, creare una copia di backup di Kaspersky Security Center Linux Administration Server utilizzando l'attività Backup dei dati di Administration Server o l'utilità klbackup e salvarla in una posizione sicura.

Nella Guida all'hardening, sono descritti i suggerimenti e le caratteristiche della configurazione di Kaspersky Security Center Linux e dei suoi componenti, intesi a ridurre i rischi di compromissione.

La Guida all'hardening contiene le seguenti informazioni:

- Selezione dell'architettura di Administration Server
- Configurazione di una connessione sicura ad Administration Server
- Configurazione degli account per l'accesso ad Administration Server
- Gestione della protezione di Administration Server

- Gestione della protezione dei dispositivi client
- Configurazione della protezione per le applicazioni gestite
- Manutenzione di Administration Server
- Trasferimento di informazioni ad applicazioni di terzi
- Suggerimenti sulla sicurezza per i sistemi informativi di terze parti

Distribuzione di Administration Server

Architettura di Administration Server

In generale, la scelta di un'architettura di gestione centralizzata dipende dalla posizione dei dispositivi protetti, dall'accesso da reti adiacenti, dagli schemi di distribuzione degli aggiornamenti del database e così via.

Nella fase iniziale dello sviluppo dell'architettura, si consiglia di familiarizzare con i componenti di Kaspersky Security Center Linux e con le modalità di interazione tra essi, così come con gli schemi per il traffico dati e l'utilizzo delle porte.

Sulla base di queste informazioni, è possibile formare un'architettura che specifichi:

- La posizione di Administration Server e le connessioni di rete
- L'organizzazione delle aree di lavoro dell'amministratore e i metodi di connessione ad Administration Server
- I metodi di distribuzione per Network Agent e il software di protezione
- L'utilizzo dei punti di distribuzione
- L'utilizzo di Administration Server virtuali
- L'utilizzo di una gerarchia di Administration Server
- Lo schema di aggiornamento del database anti-virus
- Altri flussi informativi

Selezione di un dispositivo per l'installazione di Administration Server

Si consiglia di installare Administration Server in un server dedicato nell'infrastruttura dell'organizzazione. Se nel server non è installato altro software di terzi, è possibile configurare le impostazioni di sicurezza in base ai requisiti di Kaspersky Security Center Linux, senza dipendere dai requisiti del software di terzi.

È possibile distribuire Administration Server in un server fisico o in un server virtuale. Verificare che il dispositivo selezionato soddisfi i requisiti hardware e software.

Limitazione della distribuzione di Administration Server in un controller di dominio, un server terminal o un dispositivo utente

Si sconsiglia vivamente di installare Administration Server in un controller di dominio, un server terminal o un dispositivo utente.

Si consiglia di fornire la separazione funzionale dei nodi chiave di rete. Questo approccio consente di mantenere l'operatività di diversi sistemi quando un nodo si guasta o è compromesso. Al contempo, è possibile creare diversi criteri di sicurezza per ciascun nodo.

Account per l'installazione e l'esecuzione di Administration Server

Durante la distribuzione di Administration Server, è necessario creare due account senza privilegi. I servizi inclusi in Administration Server funzioneranno con questi account senza privilegi. Seguire il principio del privilegio minimo quando si concedono diritti e autorizzazioni agli account. Evitare di includere account non necessari nel gruppo "kladmins".

È inoltre necessario creare un account DBMS interno. Administration Server utilizza questo account DBMS interno per accedere al DBMS selezionato.

Il set di account richiesti e i loro diritti dipende dal tipo di DBMS selezionato e dal metodo di creazione del database di Administration Server.

Sicurezza della connessione

Utilizzo di TLS

Si consiglia di vietare le connessioni non sicure ad Administration Server. Ad esempio, è possibile vietare le connessioni che utilizzano HTTP nelle impostazioni di Administration Server.

Si noti che, per impostazione predefinita, diverse porte HTTP di Administration Server sono chiuse. La porta rimanente viene utilizzata per il server Web di Administration Server (8060). Questa porta può essere limitata dalle impostazioni del firewall del dispositivo Administration Server.

Impostazioni TLS rigorose

Si consiglia di utilizzare il protocollo TLS versione 1.2 e successive e di limitare o vietare gli algoritmi di criptaggio non sicuri.

È possibile configurare i protocolli di criptaggio (TLS) utilizzati da Administration Server. Si noti che al momento del rilascio di una versione di Administration Server, le impostazioni del protocollo di criptaggio sono configurate per impostazione predefinita per garantire un trasferimento sicuro dei dati.

Limitazione dell'accesso al database di Administration Server

Si consiglia di limitare l'accesso al database di Administration Server. Ad esempio, concedere l'accesso solo dal dispositivo Administration Server. In questo modo, si riduce la probabilità che il database di Administration Server venga compromesso a causa di vulnerabilità note.

È possibile configurare i parametri in base alle istruzioni operative del database utilizzato, nonché fornire porte chiuse sui firewall.

Configurazione di una lista di indirizzi IP consentiti per la connessione ad Administration Server

Per impostazione predefinita, gli utenti possono accedere a Kaspersky Security Center Linux da qualsiasi dispositivo in cui è installato Kaspersky Security Center Web Console. È possibile configurare Administration Server in modo che gli utenti possano connettersi ad esso solo da dispositivi con indirizzi IP consentiti.

Account e autenticazione

Prima di eseguire i seguenti passaggi, creare una copia di backup di Kaspersky Security Center Linux Administration Server utilizzando l'attività Backup dei dati di Administration Server o l'utilità klbackup e salvarla in una posizione sicura.

Utilizzo della verifica in due passaggi con Administration Server

Kaspersky Security Center Linux fornisce la verifica in due passaggi per gli utenti di Kaspersky Security Center Web Console, basata sullo standard RFC 6238 (algoritmo TOTP, Time-based One-time Password).

Quando la verifica in due passaggi è abilitata per il proprio account, ogni volta che si accede a Kaspersky Security Center Web Console è necessario immettere il nome utente, la password e un codice di sicurezza monouso aggiuntivo. Per ricevere un codice di sicurezza monouso è necessario installare un'app di autenticazione nel computer o nel dispositivo mobile.

Esistono autenticatori software e hardware (token) che supportano lo standard RFC 6238. Ad esempio, gli autenticatori software includono Google Authenticator, Microsoft Authenticator, FreeOTP.

Si sconsiglia vivamente di installare l'app di autenticazione nello stesso dispositivo da cui viene stabilita la connessione ad Administration Server. È possibile installare un'app di autenticazione nel dispositivo mobile.

Utilizzo dell'autenticazione a due fattori per un sistema operativo

Si consiglia di utilizzare l'autenticazione a più fattori (MFA) per l'autenticazione nel dispositivo Administration Server utilizzando un token, una smart card o un altro metodo (se possibile).

Divieto di salvare la password amministratore

Se si utilizza Kaspersky Security Center Web Console, si sconsiglia di salvare la password amministratore nel browser installato nel dispositivo dell'utente.

Autenticazione di un account utente interno

Per impostazione predefinita, la password di un account utente interno di Administration Server deve rispettare le seguenti regole:

- La password deve avere una lunghezza compresa tra 8 e 16 caratteri.
- La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
  - Lettere maiuscole (A-Z)

- Lettere minuscole (a-z)
- Numeri (0-9)
- Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- La password non deve contenere spazi, caratteri Unicode o la combinazione di "." e "@", quando "." si trova prima di "@".

Per impostazione predefinita, il numero massimo di tentativi di immissione della password consentiti è 10. È possibile modificare il numero di tentativi di immissione della password consentiti.

L'utente di Kaspersky Security Center Linux può immettere una password non valida un numero limitato di volte. Una volta raggiunto il limite, l'account utente viene bloccato per un'ora.

Gruppo di amministrazione dedicato per Administration Server

Si consiglia di creare un gruppo di amministrazione dedicato per Administration Server. Concedere a questo gruppo diritti di accesso speciali e creare un criterio di sicurezza speciale per lo stesso.

Per evitare di abbassare intenzionalmente il livello di sicurezza di Administration Server, si consiglia di limitare l'elenco degli account che possono gestire il gruppo di amministrazione dedicato.

Limitazione dell'assegnazione del ruolo di amministratore principale

All'utente creato dall'utilità kladduser viene assegnato il ruolo di amministratore principale nell'elenco di controllo degli accessi (ACL) di Administration Server. Si consiglia di evitare l'assegnazione del ruolo di amministratore principale a un numero elevato di utenti.

Configurazione dei diritti di accesso alle funzionalità dell'applicazione

Si consiglia di utilizzare una configurazione flessibile dei diritti di accesso alle funzionalità di Kaspersky Security Center Linux per ciascun utente o gruppo di utenti.

Il controllo degli accessi in base al ruolo consente la creazione di ruoli utente standard con un set di diritti predefinito e l'assegnazione di tali ruoli agli utenti sulla base dell'ambito delle relative mansioni lavorative.

Principali vantaggi del modello di controllo degli accessi in base al ruolo:

- Amministrazione semplificata
- Gerarchia dei ruoli
- Approccio con privilegio minimo
- Separazione dei compiti

È possibile assegnare ruoli predefiniti a determinati dipendenti in base alle loro posizioni o creare ruoli completamente nuovi.

Durante la configurazione dei ruoli, prestare attenzione ai privilegi associati alla modifica dello stato della protezione del dispositivo Administration Server e all'installazione remota di software di terzi:

- Gestione dei gruppi di amministrazione.
- Operazioni con Administration Server.
- Installazione remota.
- Modifica dei parametri per l'archiviazione di eventi e l'invio delle notifiche.

  Questo privilegio consente di impostare notifiche che eseguono uno script o un modulo eseguibile nel dispositivo Administration Server quando si verifica un evento.

Account separato per l'installazione remota delle applicazioni

Oltre alla differenziazione di base dei diritti di accesso, si consiglia di limitare l'installazione remota delle applicazioni per tutti gli account (ad eccezione dell'amministratore principale o di un altro account specializzato).

Si consiglia di utilizzare un account separato per l'installazione remota delle applicazioni. È possibile assegnare un ruolo o autorizzazioni all'account separato.

Controllo periodico di tutti gli utenti e delle azioni degli utenti

Si consiglia di eseguire un controllo periodico di tutti gli utenti sul dispositivo Administration Server. In questo modo, è possibile rispondere a determinati tipi di minacce alla sicurezza associate alla possibile compromissione del dispositivo.

È inoltre possibile monitorare le azioni degli utenti, ad esempio la connessione e la disconnessione da Administration Server, la connessione ad Administration Server con un errore e la modifica degli oggetti (per gli oggetti che supportano la gestione delle revisioni).

Gestione della protezione di Administration Server

Selezione di un software di protezione di Administration Server

A seconda del tipo di distribuzione di Administration Server e della strategia di protezione generale, selezionare l'applicazione per proteggere il dispositivo Administration Server.

Se si distribuisce Administration Server in un dispositivo dedicato, si consiglia di selezionare l'applicazione Kaspersky Endpoint Security per proteggere il dispositivo Administration Server. In questo modo, è possibile applicare tutte le tecnologie disponibili per proteggere il dispositivo Administration Server, inclusi i moduli di analisi del comportamento.

Se Administration Server è installato in un dispositivo esistente nell'infrastruttura ed è stato utilizzato in precedenza per altre attività, si consiglia di prendere in considerazione il seguente software di protezione:

- Kaspersky Industrial CyberSecurity for Nodes. Si consiglia di installare questa applicazione nei dispositivi inclusi in una rete industriale. Kaspersky Industrial CyberSecurity for Nodes è un'applicazione che dispone di certificati di compatibilità con vari produttori di software industriale.
- Prodotti di sicurezza suggeriti. Se Administration Server è installato in un dispositivo con altro software, si consiglia di consultare i suggerimenti del fornitore del software sulla compatibilità dei prodotti di sicurezza (potrebbero già essere disponibili suggerimenti per la selezione di una soluzione di sicurezza e potrebbe essere necessario configurare l'area attendibile).

Creazione di un criterio di sicurezza separato per l'applicazione di protezione

Si consiglia di creare un criterio di sicurezza separato per l'applicazione che protegge il dispositivo Administration Server. Questo criterio deve essere diverso dal criterio di sicurezza per i dispositivi client. In questo modo, è possibile specificare le impostazioni di sicurezza più appropriate per Administration Server, senza influire sul livello di protezione di altri dispositivi.

Si consiglia di dividere i dispositivi in gruppi e quindi di inserire il dispositivo Administration Server in un gruppo separato per il quale è possibile creare criteri di sicurezza speciali.

Moduli di protezione

In assenza di suggerimenti speciali da parte del fornitore del software di terzi installato nello stesso dispositivo di Administration Server, si consiglia di attivare e configurare tutti i moduli di protezione disponibili (dopo aver verificato il funzionamento di tali moduli di protezione per un certo periodo di tempo).

Configurazione del firewall del dispositivo Administration Server

Nel dispositivo Administration Server, si consiglia di configurare il firewall in modo da limitare il numero di dispositivi da cui gli amministratori possono connettersi ad Administration Server tramite Kaspersky Security Center Web Console.

Per impostazione predefinita, Administration Server utilizza la porta 13299 per ricevere le connessioni da Kaspersky Security Center Web Console. Si consiglia di limitare il numero di dispositivi da cui è possibile gestire Administration Server utilizzando questa porta.

Gestione della protezione dei dispositivi client

Limitazione dell'aggiunta di chiavi di licenza ai pacchetti di installazione

I pacchetti di installazione sono archiviati nella cartella condivisa di Administration Server, nella sottocartella Pacchetti. Se si aggiunge una chiave di licenza a un pacchetto di installazione, tutti gli utenti con diritti di lettura su questa cartella possono accedere alla chiave di licenza (direttamente o tramite il server Web integrato in Administration Server).

Per evitare di compromettere la chiave di licenza, si sconsiglia di aggiungere chiavi di licenza ai pacchetti di installazione.

Si consiglia di utilizzare la distribuzione automatica delle chiavi di licenza ai dispositivi gestiti, la distribuzione tramite l'attività Aggiungi chiave di licenza per un'applicazione gestita e aggiungere manualmente un codice di attivazione o un file chiave ai dispositivi.

Regole automatiche per lo spostamento dei dispositivi tra i gruppi di amministrazione

Si consiglia di limitare l'uso delle regole automatiche per lo spostamento dei dispositivi tra i gruppi di amministrazione.

Se si utilizzano regole automatiche per lo spostamento dei dispositivi, ciò potrebbe comportare la propagazione di criteri che forniscono più privilegi al dispositivo spostato rispetto a quelli di cui disponeva prima del riposizionamento.

Inoltre, lo spostamento di un dispositivo client in un altro gruppo di amministrazione può comportare la propagazione delle impostazioni dei criteri. Queste impostazioni dei criteri potrebbero non essere appropriate per la distribuzione a dispositivi guest e non attendibili.

Questo suggerimento non si applica all'allocazione iniziale una tantum dei dispositivi ai gruppi di amministrazione.

Requisiti di sicurezza per i punti di distribuzione e i gateway di connessione

I dispositivi con Network Agent installato possono fungere da punto di distribuzione ed eseguire le seguenti funzioni:

- Distribuire gli aggiornamenti e i pacchetti di installazione ricevuti da Administration Server ai dispositivi client all'interno del gruppo.
- Eseguire l'installazione remota di software di terzi e applicazioni Kaspersky nei dispositivi client.
- Eseguire il polling della rete per rilevare nuovi dispositivi e aggiornare le informazioni sui dispositivi esistenti. Il punto di distribuzione può utilizzare gli stessi metodi di rilevamento dei dispositivi di Administration Server.

Posizionamento dei punti di distribuzione sulla rete dell'organizzazione utilizzati per:

- Riduzione del carico su Administration Server
- Ottimizzazione del traffico
- Concessione all'Administration Server dell'accesso ai dispositivi in parti difficili da raggiungere della rete

Tenendo conto delle capacità disponibili, si consiglia di proteggere i dispositivi che fungono da punti di distribuzione da qualsiasi tipo di accesso non autorizzato (anche fisico).

Limitazione dell'assegnazione automatica dei punti di distribuzione

Per semplificare l'amministrazione e assicurare l'operatività della rete, si consiglia di utilizzare l'assegnazione automatica dei punti di distribuzione. Tuttavia, per le reti industriali e le reti di piccole dimensioni, si consiglia di evitare l'assegnazione automatica dei punti di distribuzione, poiché, ad esempio, le informazioni private degli account utilizzati per il push delle attività di installazione remota possono essere trasferite ai punti di distribuzione tramite il sistema operativo.

Per le reti industriali e le reti di piccole dimensioni, è possibile assegnare manualmente i dispositivi in modo che fungano da punti di distribuzione.

È inoltre possibile visualizzare il Rapporto sull'attività dei punti di distribuzione.

Configurazione della protezione per le applicazioni gestite

Criteri delle applicazioni gestite

Si consiglia di creare un criterio per ogni tipo di applicazione e componente utilizzato di Kaspersky Security Center Linux (Network Agent, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security for Linux, Kaspersky Endpoint Agent e altri). Questo criterio deve essere applicato a tutti i dispositivi gestiti (il gruppo di amministrazione principale) o a un gruppo separato in cui i nuovi dispositivi gestiti vengono automaticamente spostati in base alle regole di spostamento configurate.

Indicazione della password per disabilitare la protezione e disinstallare l'applicazione

Si consiglia vivamente di abilitare la protezione con password per impedire agli intrusi di disabilitare o disinstallare le applicazioni di protezione Kaspersky. Nelle piattaforme in cui è supportata la protezione con password, è possibile impostare la password, ad esempio, per Kaspersky Endpoint Security, Network Agent e altre applicazioni Kaspersky. Dopo aver abilitato la protezione tramite password, si consiglia di bloccare le impostazioni corrispondenti chiudendo il "lucchetto".

Specificazione della password per la connessione manuale di un dispositivo client ad Administration Server (utilità klmover)

L'utilità klmover consente di connettere manualmente un dispositivo client ad Administration Server. L'utilità klmover si trova nella cartella di installazione di Network Agent.

Per impedire agli intrusi di spostare i dispositivi fuori dal controllo di Administration Server, si consiglia di abilitare la protezione tramite password per l'esecuzione dell'utilità klmover. Per abilitare la protezione con password, selezionare l'opzione **Usa password di disinstallazione** nelle impostazioni dei criteri di Network Agent.

L'utilità klmover richiede i diritti di amministratore locale.

Se si perde o si dimentica la password di Network Agent protetto da password installato nel dispositivo che non è più sotto la gestione di Kaspersky Security Center Linux, non è possibile rimuovere Network Agent utilizzando l'utilità klmover o il prompt dei comandi. In questo caso, è necessario reinstallare il sistema operativo nel dispositivo in cui è installato Network Agent protetto da password.

L'abilitazione dell'opzione **Usa password di disinstallazione** nei dispositivi Windows consente anche di abilitare la protezione tramite password per lo strumento Cleaner (cleaner.exe).

Utilizzo di Kaspersky Security Network

In tutti i criteri delle applicazioni gestite e nelle proprietà di Administration Server, si consiglia di abilitare l'uso di Kaspersky Security Network (KSN) e di accettare l'Informativa KSN. Quando si aggiorna o si effettua l'upgrade di Administration Server, è possibile accettare l'Informativa KSN aggiornata. In alcuni casi, quando l'uso dei servizi cloud è vietato dalla legge o da altri regolamenti, è possibile disabilitare KSN.

Scansione regolare dei dispositivi gestiti

Per tutti i gruppi di dispositivi, si consiglia di creare un'attività che esegua periodicamente una scansione completa dei dispositivi.

Individuazione di nuovi dispositivi

Si consiglia di configurare correttamente le impostazioni di rilevamento dei dispositivi: impostare l'integrazione con controller di dominio e specificare gli intervalli di indirizzi IP per il rilevamento di nuovi dispositivi.

Per motivi di sicurezza, è possibile utilizzare il gruppo di amministrazione predefinito che include tutti i nuovi dispositivi e i criteri predefiniti che interessano questo gruppo.

Manutenzione di Administration Server

Copia di backup dei dati di Administration Server

Backup dei dati consente di ripristinare i dati di Administration Server senza perdita di dati.

Per impostazione predefinita, un'attività di backup dei dati viene creata automaticamente dopo l'installazione di Administration Server e viene eseguita periodicamente, salvando i backup nella directory appropriata.
Le impostazioni dell'attività di backup dei dati possono essere modificate come segue:

- La frequenza di backup aumenta
- Viene specificata una directory speciale per il salvataggio delle copie
- Le password per le copie di backup sono state modificate

Se si archiviano copie di backup in una directory speciale, diversa dalla directory predefinita, si consiglia di limitare l'elenco di controllo di accesso (ACL, Access Control List) per questa directory. Gli account di Administration Server e gli account del database di Administration Server devono disporre dell'accesso in scrittura per questa directory.

Manutenzione di Administration Server

La manutenzione di Administration Server consente di ridurre il volume del database e migliorare le prestazioni e l'affidabilità delle operazioni dell'applicazione. È consigliabile eseguire la manutenzione di Administration Server almeno ogni settimana.

La manutenzione di Administration Server viene eseguita tramite un'attività specializzata. Durante la manutenzione di Administration Server, l'applicazione esegue le azioni seguenti:

- Riorganizza gli indici del database
- Aggiorna le statistiche del database
- Riduce le dimensioni del database (se necessario)

Installazione degli aggiornamenti del sistema operativo e degli aggiornamenti software di terzi

Si consiglia vivamente di installare periodicamente gli aggiornamenti software per il sistema operativo e il software di terzi nel dispositivo Administration Server.

I dispositivi client non richiedono una connessione continua ad Administration Server, quindi è possibile riavviare il dispositivo Administration Server in modo sicuro dopo aver installato gli aggiornamenti. Tutti gli eventi registrati nei dispositivi client durante il periodo di inattività di Administration Server vengono inviati ad esso dopo il ripristino della connessione.

Trasferimento di eventi a sistemi di terzi

Monitoraggio e generazione dei rapporti

Per una risposta tempestiva ai problemi di sicurezza, si consiglia di configurare le funzionalità di monitoraggio e generazione dei rapporti.

Esportazione di eventi nei sistemi SIEM

Per il rilevamento rapido dei problemi di sicurezza prima che si verifichino danni significativi, si consiglia di utilizzare l'esportazione degli eventi in un sistema SIEM.

Notifiche e-mail degli eventi di controllo

Kaspersky Security Center Linux consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Per una risposta tempestiva alle emergenze, si consiglia di configurare Administration Server in modo che invii notifiche sugli eventi di controllo, gli eventi critici, gli eventi di errore e gli avvisi pubblicati.

Poiché questi eventi sono eventi interni al sistema, è prevedibile che se ne verifichino pochi; si tratta di una situazione abbastanza normale per la posta.

Scenario: autenticazione di MySQL Server

Si consiglia di utilizzare un certificato TLS per autenticare MySQL Server. È possibile utilizzare un certificato di un'autorità di certificazione attendibile o un certificato autofirmato.

Administration Server supporta l'autenticazione SSL unidirezionale e bidirezionale per MySQL.

Abilitazione dell'autenticazione SSL unidirezionale

Seguire questi passaggi per configurare l'autenticazione SSL unidirezionale per MySQL:

1. **Generare un certificato TLS autofirmato per il server MySQL**

   Eseguire il seguente comando:

   ```
   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. **Creare un file flag del server**

Utilizzare l'utilità klscflag per creare il contrassegno del server KLSRV_MYSQL_OPT_SSL_CA e specificare il percorso del certificato come valore. L'utilità klscflag si trova nella directory in cui è installato Administration Server. Il percorso di installazione predefinito è /opt/kaspersky/ksc64/sbin.

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

3. **Configurare il database**

   Specificare i certificati nel file my.cnf. Aprire il file my.cnf in un editor di testo e aggiungere le seguenti righe nella sezione [mysqld]:

   ```
   [mysqld]

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

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

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

Abilitazione dell'autenticazione SSL bidirezionale

Seguire questi passaggi per configurare l'autenticazione SSL bidirezionale per MySQL:

1. **Creare file flag del server**

   Utilizzare l'utilità klscflag per creare i contrassegni del server e specificare il percorso dei file del certificato come valori:

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

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

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

   L'utilità klscflag si trova nella directory in cui è installato Administration Server. Il percorso di installazione predefinito è /opt/kaspersky/ksc64/sbin.

2. **Specificare la passphrase (facoltativo)**

   Se server-key.pem richiede una passphrase, creare un contrassegno KLSRV_MARIADB_OPT_TLS_PASPHRASE e specificare la passphrase come valore:

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

3. **Configurare il database**

   Specificare i certificati nel file my.cnf. Aprire il file my.cnf in un editor di testo e aggiungere le seguenti righe nella sezione [mysqld]:

   ```
   [mysqld]

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

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

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

Scenario: autenticazione del server PostgreSQL

Si consiglia di utilizzare un certificato TLS per autenticare il server PostgreSQL. È possibile utilizzare un certificato di un'autorità di certificazione attendibile o un certificato autofirmato.

Administration Server supporta l'autenticazione SSL unidirezionale e bidirezionale per PostgreSQL.

L'autenticazione del server PostgreSQL avviene in fasi:

1. **Generazione di un certificato per il server PostgreSQL**

   Eseguire i seguenti comandi:

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

   ```
   chmod og-rwx psql.key
   ```

2. **Generazione di un certificato per Administration Server**

   Eseguire i seguenti comandi. Il valore CN deve corrispondere al nome dell'utente che si connette a PostgreSQL per conto di Administration Server. Il nome utente è impostato su postgres per impostazione predefinita.

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

   ```
   chmod og-rwx postgres.key
   ```

3. **Configurazione dell'autenticazione del certificato client**

   Modificare pg_hba.conf come segue:

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

   Assicurarsi che pg_hba.conf non includa un record che inizia con `host`.

4. **Specifica del certificato PostgreSQL**

   Autenticazione SSL unidirezionale

   Modificare postgresql.conf come segue (specificare il percorso corretto dei file .crt e .key):

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

   Autenticazione SSL bidirezionale

   Modificare postgresql.conf come segue (specificare il percorso corretto dei file .crt e .key):

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

5. **Riavvio del daemon PostgreSQL**

   Eseguire il seguente comando:

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

6. **Specifica del flag del server per Administration Server**

   Autenticazione SSL unidirezionale

   Utilizzare l'utilità klscflag per creare il contrassegno del server KLSRV_POSTGRES_OPT_SSL_CA e specificare il percorso del certificato come valore.

   Eseguire la riga dei comandi, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella directory in cui è installato Administration Server. Il percorso di installazione predefinito è /opt/kaspersky/ksc64/sbin.

   Eseguire il seguente comando:

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

   Autenticazione SSL bidirezionale

   Utilizzare l'utilità klscflag per creare i contrassegni del server e specificare il percorso dei file del certificato come valori.

   Eseguire la riga dei comandi, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella directory in cui è installato Administration Server. Il percorso di installazione predefinito è /opt/kaspersky/ksc64/sbin.

   Eseguire i seguenti comandi:

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

   Se `postgres.key` richiede una passphrase, creare un contrassegno KLSRV_POSTGRES_OPT_TLS_PASPHRASE e specificare la passphrase come valore:

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

7. **Riavvio del servizio Administration Server**

Preparazione per la distribuzione

Questa sezione descrive le operazioni che è necessario eseguire prima della distribuzione di Kaspersky Security Center Linux.

Pianificazione della distribuzione di Kaspersky Security Center Linux

Questa sezione contiene informazioni sulle opzioni più convenienti per la distribuzione dei componenti di Kaspersky Security Center Linux nella rete di un'organizzazione a seconda dei seguenti criteri:

- Numero totale di dispositivi

- Unità (sedi locali, filiali) separate a livello organizzativo o geografico
- Reti distinte connesse tramite canali con larghezza di banda ridotta
- Necessità dell'accesso via Internet all'Administration Server

Schemi tipici di distribuzione di un sistema di protezione

In questa sezione vengono descritti gli schemi standard per la distribuzione di un sistema di protezione anti-virus in una rete aziendale tramite Kaspersky Security Center.

Il sistema deve essere protetto contro qualsiasi tipo di accesso non autorizzato. È consigliabile installare tutti gli aggiornamenti della protezione disponibili per il sistema operativo prima di installare l'applicazione nel dispositivo e proteggere fisicamente Administration Server e punti di distribuzione.

È possibile utilizzare Kaspersky Security Center per distribuire un sistema di protezione in una rete aziendale tramite i seguenti schemi di distribuzione:

- Distribuzione di un sistema di protezione tramite Kaspersky Security Center Web Console.

  Le applicazioni Kaspersky vengono installate automaticamente nei dispositivi client che, a loro volta, vengono connessi automaticamente ad Administration Server utilizzando Kaspersky Security Center.

- Distribuzione manuale di un sistema di protezione utilizzando pacchetti di installazione indipendenti generati da Kaspersky Security Center.

  L'installazione delle applicazioni Kaspersky nei dispositivi client e nella workstation dell'amministratore viene eseguita manualmente; le impostazioni per la connessione dei dispositivi client ad Administration Server vengono specificate durante l'installazione di Network Agent.

  Questo metodo di distribuzione è consigliato nei casi in cui l'installazione remota non è possibile.

Kaspersky Security Center non supporta la distribuzione utilizzando i criteri di gruppo di Microsoft Active Directory®.

Informazioni sulla pianificazione della distribuzione di Kaspersky Security Center Linux nella rete di un'organizzazione

Un Administration Server può supportare un massimo di 50.000 dispositivi (con PostgreSQL o Postgres Pro come DBMS). Se il numero totale di dispositivi nella rete di un'organizzazione è superiore a 50.000, è necessario distribuire più Administration Server nella rete e combinarli in una gerarchia per gestirli comodamente in modo centralizzato.

Se un'organizzazione include sedi locali remote su larga scala (filiali) con amministratori distinti, è consigliabile distribuire gli Administration Server in tali sedi. In caso contrario, tali filiali devono essere considerate reti distinte connesse tramite canali a basso throughput; vedere la sezione "Configurazione standard: poche sedi su larga scala gestite da amministratori distinti".

Quando si utilizzano reti distinte connesse tramite canali con larghezza di banda ridotta, è possibile ridurre il traffico assegnando a uno o più Network Agent il ruolo di punto di distribuzione (vedere la tabella per il calcolo del numero di punti di distribuzione). In questo caso, tutti i dispositivi in una rete distinta recupereranno gli aggiornamenti da tali centri di aggiornamento locali. I punti di distribuzione effettivi possono scaricare gli aggiornamenti sia da Administration Server (scenario predefinito) sia dai server Kaspersky in Internet (vedere la sezione "Configurazione standard: più sedi remote di piccole dimensioni").

La sezione "Configurazioni standard di Kaspersky Security Center Linux" fornisce descrizioni dettagliate delle configurazioni standard di Kaspersky Security Center Linux. Durante la pianificazione della distribuzione, scegliere la configurazione standard più adatta, in base alla struttura dell'organizzazione.

In fase di pianificazione della distribuzione, deve essere valutata l'assegnazione di uno speciale certificato X.509 all'Administration Server. L'assegnazione del certificato X.509 all'Administration Server può essere utile nei seguenti casi (elenco parziale):

- Ispezione del traffico SSL (Secure Sockets Layer) per mezzo di un proxy con terminazione SSL o per l'utilizzo di un proxy inverso
- Specificazione dei valori richiesti nei campi del certificato
- Specificazione del livello di criptaggio richiesto di un certificato

Selezione di una struttura per la protezione di un'azienda

La selezione di una struttura per la protezione di un'organizzazione viene definita dai seguenti fattori:

- Topologia della rete dell'organizzazione.
- Struttura dell'organizzazione.
- Numero di dipendenti responsabili della protezione della rete e allocazione delle relative responsabilità.
- Risorse hardware che possono essere allocate nei componenti di gestione della protezione.
- Throughput dei canali di comunicazione che è possibile allocare per la manutenzione dei componenti della protezione nella rete dell'organizzazione.
- Limiti di tempo per l'esecuzione di operazioni amministrative critiche nella rete dell'organizzazione. Le operazioni amministrative critiche includono, ad esempio, la distribuzione dei database anti-virus e la modifica dei criteri per i dispositivi client.

Quando si seleziona una struttura di protezione, è innanzitutto consigliabile effettuare una stima delle risorse hardware e di rete disponibili che è possibile utilizzare per l'esecuzione di un sistema di protezione centralizzato.

Per analizzare l'infrastruttura di rete e hardware, è consigliabile attenersi alla seguente procedura:

1. Definire le seguenti impostazioni della rete per cui verrà distribuita la protezione:
   - Numero di segmenti di rete.
   - Velocità dei canali di comunicazione tra i singoli segmenti di rete.
   - Numero di dispositivi gestiti in ciascun segmento di rete.

- Throughput di ciascun canale di comunicazione che è possibile allocare per garantire il funzionamento della protezione.

2. Determinare il tempo massimo consentito per l'esecuzione delle operazioni di amministrazione chiave per tutti i dispositivi gestiti.

3. Analizzare le informazioni dei passaggi 1 e 2, oltre ai dati dai test di carico del sistema di amministrazione. In base all'analisi, rispondere alle seguenti domande:

   - È possibile servire tutti i client con un solo Administration Server o è necessaria una gerarchia di Administration Server?

   - Quale configurazione hardware di Administration Server è necessaria per gestire tutti i client nel rispetto dei limiti di tempo specificati al passaggio 2?

   - È necessario utilizzare i punti di distribuzione per ridurre il carico sui canali di comunicazione?

Dopo aver ottenuto le risposte alle domande indicate nel passaggio 3, è possibile compilare un set di strutture consentite per la protezione dell'organizzazione.

Nella rete dell'organizzazione è possibile utilizzare una delle seguenti strutture di protezione standard:

- Un solo Administration Server. Tutti i dispositivi client sono connessi a un solo Administration Server. Administration Server opera come punto di distribuzione.

- Un solo Administration Server con punti di distribuzione. Tutti i dispositivi client sono connessi a un solo Administration Server. Alcuni dispositivi client della rete operano come punti di distribuzione.

- Gerarchia di Administration server. Per ciascun segmento di rete viene allocato un singolo Administration Server, che entra a far parte di una gerarchia generale di Administration Server. L'Administration Server primario opera come punto di distribuzione.

- Gerarchia di Administration Server con punti di distribuzione. Per ciascun segmento di rete viene allocato un singolo Administration Server, che entra a far parte di una gerarchia generale di Administration Server. Alcuni dispositivi client della rete operano come punti di distribuzione.

Configurazioni standard di Kaspersky Security Center Linux

Questa sezione descrive le seguenti configurazioni standard utilizzate per la distribuzione dei componenti di Kaspersky Security Center Linux nella rete di un'organizzazione:

- Singola sede

- Poche sedi su larga scala, separate a livello geografico e gestite da amministratori distinti

- Più sedi di piccole dimensioni, separate a livello geografico

Configurazione standard: singola sede

È possibile distribuire uno o più Administration Server nella rete dell'organizzazione. Il numero di Administration Server che è possibile selezionare può essere basato sull'hardware disponibile o sul numero totale di dispositivi gestiti.

Un Administration Server può supportare fino a 50.000 dispositivi (con PostgreSQL o Postgres Pro come DBMS). Considerare la possibilità di aumentare il numero di dispositivi gestiti in futuro: può essere utile connettere un numero più limitato di dispositivi a un singolo Administration Server.

Gli Administration Server possono essere distribuiti nella rete interna o nella rete perimetrale, a seconda del fatto che sia necessario o meno l'accesso via Internet agli Administration Server.

Se vengono utilizzati più server, è consigliabile combinarli in una gerarchia. L'utilizzo di una gerarchia di Administration Server consente di evitare la duplicazione di criteri e attività e di amministrare l'intero set di dispositivi gestiti come se fossero gestiti da un singolo Administration Server (ricerca di dispositivi, creazione di selezioni di dispositivi e generazione di rapporti).

Configurazione standard: poche sedi su larga scala gestite da amministratori distinti

Se un'organizzazione ha diverse sedi su larga scala e geograficamente distanti, è necessario prendere in considerazione l'opzione di distribuire Administration Server in ciascuna sede. Per ogni sede possono essere distribuiti uno o più server di amministrazione, a seconda del numero di dispositivi client e dell'hardware disponibile. In questo caso, ciascuna sede avrà le caratteristiche descritte nello scenario "Configurazione standard: singola sede". Per semplificare l'amministrazione è consigliabile combinare tutti gli Administration Server in una gerarchia (possibilmente multi-livello).

Se alcuni dipendenti si spostano da un ufficio all'altro con i propri dispositivi (laptop), creare profili di connessione di Network Agent nel criterio di Network Agent. Si noti che i profili di connessione di Network Agent sono supportati solo per i dispositivi Windows e macOS.

Configurazione standard: più sedi remote di piccole dimensioni

Questa configurazione standard prevede una sede centrale e diverse sedi remote di piccole dimensioni che possono comunicare con la sede centrale tramite Internet. Ogni sede remota può essere posizionata dietro un NAT (Network Address Translation), quindi non è possibile stabilire alcuna connessione tra due sedi remote poiché sono isolate.

È necessario distribuire un Administration Server nella sede centrale e assegnare uno o più punti di distribuzione a tutte le altre sedi. Se le sedi sono collegate via Internet, può essere utile creare un'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione per i punti di distribuzione*, in modo gli aggiornamenti vengano scaricati direttamente dai server di Kaspersky, dalla cartella locale o di rete, invece che da Administration Server.

Se alcuni dispositivi in una sede remota non hanno accesso diretto all'Administration Server (ad esempio, l'accesso all'Administration Server viene fornito via Internet ma alcuni dispositivi non hanno accesso a Internet), i punti di distribuzione devono essere impostati in modalità gateway di connessione. In questo caso, i Network Agent nei dispositivi della sede remota saranno connessi per l'ulteriore sincronizzazione all'Administration Server, ma attraverso il gateway, non direttamente.

Poiché in genere l'Administration Server non è in grado di eseguire il polling della rete della sede remota, può essere utile assegnare questa funzione a un punto di distribuzione.

L'Administration Server non potrà inviare notifiche tramite la porta UDP 15000 ai dispositivi gestiti posizionati dietro il NAT nella sede remota. Per risolvere questo problema, è possibile abilitare la modalità di connessione continua ad Administration Server nelle proprietà dei dispositivi che operano come punti di distribuzione (casella di controllo **Non eseguire la disconnessione da Administration Server**). Questa modalità è disponibile se il numero totale di punti di distribuzione non è superiore a 300. Utilizzare i server push per assicurarsi che vi sia una connettività costante tra un dispositivo gestito e l'Administration Server. Fare riferimento al seguente argomento per i dettagli: Abilitazione di un server push.

Selezione di un DBMS

Nella seguente tabella, sono elencate le opzioni DBMS valide, nonché i suggerimenti e le limitazioni per il relativo utilizzo.

Suggerimenti e limitazioni su DBMS

DBMS	Suggerimenti e limitazioni
MySQL (vedere le versioni supportate)	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 20.000 dispositivi.
MariaDB (vedere le versioni supportate)	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 20.000 dispositivi.
PostgreSQL, Postgres Pro (vedere le versioni supportate)	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 50.000 dispositivi.

Per informazioni su come installare il DBMS selezionato, consultare la relativa documentazione.

Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate.

Se si decide di installare il DBMS di PostgreSQL o Postgres Pro, assicurarsi di aver specificato una password per il l'utente con privilegi avanzati. Se la password non viene specificata, Administration Server potrebbe non essere in grado di connettersi al database.

Se si installa MySQL, MariaDB, PostgreSQL o Postgres Pro, utilizzare le impostazioni consigliate per garantire il corretto funzionamento del DBMS.

Se si utilizza un DBMS PostgreSQL, MariaDB o MySQL, la scheda **Eventi** potrebbe mostrare un elenco incompleto di eventi per il dispositivo client selezionato. Questo si verifica quando il DBMS archivia una quantità molto elevata di eventi. È possibile aumentare il numero di eventi visualizzati effettuando una delle seguenti operazioni:

- Rimozione degli eventi non necessari.
- Riduzione del periodo di archiviazione per gli eventi non necessari.

Per visualizzare un elenco completo degli eventi registrati in Administration Server per il dispositivo, utilizzare Rapporti.

Concessione dell'accesso via Internet all'Administration Server

L'accesso via Internet all'Administration Server è necessario nei seguenti casi:

- Aggiornamento periodico dei database, dei moduli software e delle applicazioni Kaspersky
- Aggiornamento di software di terze parti

  Per impostazione predefinita, non è richiesta la connessione Internet per l'installazione degli aggiornamenti software Microsoft nei dispositivi gestiti da parte di Administration Server. I dispositivi gestiti possono ad esempio scaricare gli aggiornamenti software Microsoft direttamente dai server Microsoft Update o da Windows Server con Microsoft Windows Server Update Services (WSUS) distribuito nella rete dell'organizzazione. Administration Server deve essere connesso a Internet nei seguenti casi:

- Quando si usa Administration Server come server WSUS
- Per installare gli aggiornamenti di software di terze parti diverso dal software Microsoft

- Correzione delle vulnerabilità del software di terze parti

  È necessaria una connessione Internet affinché Administration Server esegua le seguenti attività:

  - Per creare un elenco di correzioni consigliate per le vulnerabilità del software Microsoft. L'elenco viene creato e aggiornato regolarmente dagli specialisti Kaspersky.
  - Per correggere le vulnerabilità in software di terze parti diverso dal software Microsoft.

- Gestione dei dispositivi (portatili) degli utenti fuori sede
- Gestione dei dispositivi nelle sedi remote
- Interazione con gli Administration Server primari o secondari situati nelle sedi remote
- Gestione dei dispositivi mobili

Questa sezione descrive i modi tipici per fornire l'accesso via Internet all'Administration Server. Ciascuno dei casi che prevedono l'accesso via Internet ad Administration Server può richiedere un certificato dedicato per Administration Server.

Accesso a Internet: Administration Server in una rete locale

Se l'Administration Server è posizionato nella rete interna di un'organizzazione, è consigliabile rendere la porta TCP 13000 dell'Administration Server accessibile dall'esterno per mezzo del port forwarding.

Accesso a Internet: Administration Server in una rete perimetrale

Se l'Administration Server è posizionato nella rete perimetrale dell'organizzazione, non ha accesso alla rete interna dell'organizzazione. Si applicano pertanto le seguenti limitazioni:

- L'Administration Server non può rilevare nuovi dispositivi.
- Administration Server non può eseguire la distribuzione iniziale di Network Agent tramite l'installazione forzata sui dispositivi nella rete interna dell'organizzazione.

  Questo vale solo per l'installazione iniziale di Network Agent. Qualsiasi ulteriore upgrade di Network Agent o l'installazione dell'applicazione di protezione potranno comunque essere eseguiti dall'Administration Server.

Si noti che Kaspersky Security Center Linux non supporta la distribuzione utilizzando i criteri di gruppo di Microsoft Windows.

È possibile utilizzare i punti di distribuzione che si trovano nella rete dell'organizzazione. Per eseguire la distribuzione iniziale nei dispositivi senza Network Agent, installare Network Agent in uno dei dispositivi e quindi assegnargli lo stato di punto di distribuzione. L'installazione iniziale di Network Agent negli altri dispositivi sarà eseguita da Administration Server tramite questo punto di distribuzione.

Per assicurare il corretto invio delle notifiche alla porta UDP 15000 sui dispositivi gestiti nella rete interna dell'organizzazione, è necessario coprire l'intera rete con punti di distribuzione. Nelle proprietà dei punti di distribuzione assegnati selezionare la casella di controllo **Non eseguire la disconnessione da Administration Server**. Administration Server stabilirà una connessione continua ai punti di distribuzione e questi potranno inviare notifiche alla porta UDP 15000 nei dispositivi che si trovano nella rete interna dell'organizzazione (può trattarsi di una rete IPv4 o IPv6).

Informazioni sui punti di distribuzione

Un dispositivo in cui è installato Network Agent può essere utilizzato come punto di distribuzione. In questa modalità, Network Agent può distribuire gli aggiornamenti, che possono essere recuperati da Administration Server o dai server Kaspersky. In quest'ultimo caso, configurare il download degli aggiornamenti per un punto di distribuzione.

La distribuzione dei punti di distribuzione nella rete di un'organizzazione ha i seguenti obiettivi:

- Riduzione del carico sull'Administration Server.
- Ottimizzazione del traffico.
- Concessione all'Administration Server dell'accesso ai dispositivi in posizioni difficili da raggiungere della rete dell'organizzazione. La disponibilità di un punto di distribuzione nella rete dietro un NAT (in relazione all'Administration Server) consente all'Administration Server di eseguire le seguenti azioni:
  - Inviare notifiche ai dispositivi tramite UDP nella rete IPv4 o IPv6
  - Eseguire il polling della rete IPv4 o IPv6
  - Eseguire la distribuzione iniziale
  - Fungere da server push

Un punto di distribuzione viene assegnato a un gruppo di amministrazione. In questo caso, l'ambito del punto di distribuzione include tutti i dispositivi all'interno del gruppo di amministrazione e di tutti i relativi sottogruppi. Tuttavia, il dispositivo che opera come punto di distribuzione può non essere incluso nel gruppo di amministrazione a cui è stato assegnato.

È possibile far funzionare un punto di distribuzione come gateway di connessione. In questo caso, i dispositivi nell'ambito del punto di distribuzione saranno connessi all'Administration Server tramite il gateway, non direttamente. Questa modalità può essere utile negli scenari che non consentono di stabilire una connessione diretta tra Administration Server e dispositivi gestiti.

Se si utilizza un dispositivo basato su Linux come punto di distribuzione, si consiglia vivamente di aumentare il limite dei descrittori di file per il servizio klnagent, poiché se l'ambito del punto di distribuzione include molti dispositivi, il numero massimo predefinito di file che è possibile aprire potrebbe non essere sufficiente.

Aumento del limite dei descrittori di file per il servizio klnagent

Se l'ambito di un punto di distribuzione basato su Linux include molti dispositivi, il limite predefinito di file che è possibile aprire (descrittori di file) potrebbe non essere sufficiente. Per evitare questo, è possibile aumentare il limite dei descrittori di file per il servizio klnagent.

Per aumentare il limite dei descrittori di file per il servizio klnagent:

1. Nel dispositivo basato su Linux che funge da punto di distribuzione, aprire il file `/lib/systemd/system/klnagent64.service`, quindi specificare i limiti hard e soft dei descrittori di file nel parametro `LimitNOFILE` della sezione `[Service]`:

   `LimitNOFILE=<soft_resource_limit>:<hard_resource_limit>`

   Ad esempio, `LimitNOFILE=32768:131072`. Si noti che il limite soft dei descrittori di file deve essere inferiore o uguale al limite hard.

2. Eseguire il seguente comando per assicurarsi che i parametri siano specificati correttamente:

   `systemd-analyze verify klnagent64.service`

   Se i parametri sono specificati in modo errato, questo comando può generare uno dei seguenti errori:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Se si verifica questo errore, i simboli nella riga `LimitNOFILE` sono stati specificati in modo errato. È necessario controllare e correggere la riga immessa.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Se si verifica questo errore, il limite soft dei descrittori di file immessi è maggiore del limite hard. È necessario controllare la riga immessa e assicurarsi che il limite soft dei descrittori di file sia uguale o inferiore al limite hard.

3. Eseguire il seguente comando per ricaricare il processo systemd:

   `systemctl daemon-reload`

4. Eseguire il seguente comando per riavviare il servizio Network Agent:

   `systemctl restart klnagent`

5. Eseguire il seguente comando per assicurarsi che i parametri specificati vengano applicati correttamente:

   `less /proc/<nagent_proc_id>/limits`

   dove il parametro `<nagent_proc_id>` è l'identificatore del processo di Network Agent. È possibile eseguire il seguente comando per ottenere l'identificatore:

   `ps -ax | grep klnagent`

Per il punto di distribuzione basato su Linux, il limite di file che è possibile aprire è stato aumentato.

Calcolo del numero e configurazione dei punti di distribuzione

Più dispositivi client contiene una rete, maggiore è il numero dei punti di distribuzione richiesti. È consigliabile non disabilitare l'assegnazione automatica dei punti di distribuzione. Quando è abilitata l'assegnazione automatica dei punti di distribuzione, Administration Server assegna i punti di distribuzione se il numero dei dispositivi client è ampio e definisce la configurazione.

Utilizzo di punti di distribuzione assegnati in modo esclusivo

Se si prevede di utilizzare alcuni dispositivi specifici come punti di distribuzione (ovvero, server assegnati in modo esclusivo), è possibile scegliere di non utilizzare l'assegnazione automatica dei punti di distribuzione. In questo caso, verificare che i dispositivi a cui assegnare il ruolo di punti di distribuzione dispongano di un volume sufficiente di spazio libero su disco, che non vengano arrestati regolarmente e che la modalità di sospensione sia disabilitata.

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–100	1
Più di 100	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Utilizzo di dispositivi client standard (workstation) come punti di distribuzione

Se si prevede di utilizzare dispositivi client standard (ovvero, workstation) come punti di distribuzione, è consigliabile assegnare i punti di distribuzione come indicato nelle tabelle seguenti per evitare un carico eccessivo sui canali di comunicazione e su Administration Server:

Numero di workstation che operano come punti di distribuzione in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Numero di workstation che operano come punti di distribuzione in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–30	1
31–300	2
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Se un punto di distribuzione viene arrestato (o non è disponibile per altri motivi), i dispositivi gestiti nel relativo ambito possono accedere ad Administration Server per gli aggiornamenti.

Administration Server virtuali

Sulla base di un Administration Server fisico, è possibile creare più Administration Server virtuali, simili agli Administration Server secondari. Rispetto al modello di accesso discrezionale, che è basato su elenchi di controllo di accesso (ACL), il modello degli Administration Server virtuali è più funzionale e fornisce un maggior livello di isolamento. Oltre a una struttura dedicata di gruppi di amministrazione per i dispositivi assegnati con criteri e attività, ogni Administration Server virtuale dispone di un proprio gruppo di dispositivi non assegnati, di insiemi di rapporti, dispositivi ed eventi selezionati, pacchetti di installazione, regole di spostamento e così via. L'ambito funzionale degli Administration Server virtuali può essere utilizzato sia dai provider di servizi (xSP) per massimizzare l'isolamento dei clienti, sia da organizzazioni su vasta scala con flussi di lavoro sofisticati e numerosi amministratori.

Gli Administration Server virtuali sono molto simili agli Administration Server secondari, ma con le seguenti distinzioni:

- Un Administration Server virtuale non dispone della maggior parte delle impostazioni globali e di specifiche porte TCP.
- Un Administration Server virtuale non dispone di Administration Server secondari.
- Un Administration Server virtuale non include altri Administration Server virtuali.
- Un Administration Server fisico visualizza i dispositivi, i gruppi, gli eventi e gli oggetti nei dispositivi gestiti (elementi in Quarantena, registro delle applicazioni e così via) di tutti i relativi Administration Server virtuali.
- Un Administration Server virtuale può eseguire solo la scansione della rete a cui sono connessi punti di distribuzione.

Impostazioni di rete per l'interazione con servizi esterni

Kaspersky Security Center Linux utilizza le seguenti impostazioni di rete per l'interazione con i servizi esterni.

Impostazioni di rete

Impostazioni di rete	Indirizzo	Descrizione
Porta: 443 Protocollo: HTTPS	activation-v2.kaspersky.com/activationservice/activationservice.svc	Attivazione dell'applicazione.
Porta: 443 Protocollo: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky.
Porta: 443 Protocollo: HTTPS	https://downloads.upd.kaspersky.com	• Aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky. • Verifica dell'accessibilità dei server Kaspersky. Prima di scaricare i database e i moduli software di Kaspersky, Kaspersky Security Center Linux verifica se i server Kaspersky sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici.

Porta: 80 Protocollo: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky.
Porta: 443 Protocollo: HTTPS	ds.kaspersky.com	Utilizzo di Kaspersky Security Network.
Porto: 443, 1443 Protocollo: 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	Utilizzo di Kaspersky Security Network.
Protocollo: HTTPS	click.kaspersky.com redirect.kaspersky.com	Visita dei collegamenti sull'interfaccia.
Porta: 80 Protocollo: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Questi server fanno parte della Public Key Infrastructure (PKI) e sono necessari per verificare lo stato di validità dei certificati di firma digitale Kaspersky. Il CRL è un elenco di certificati revocati. L'OCSP consente di richiedere lo stato di uno specifico certificato in tempo reale. Questi server aiutano a garantire la sicurezza dell'interazione con i certificati digitali e a proteggersi da possibili attacchi.
Porta: 443 Protocollo: HTTPS	https://ipm-klca.kaspersky.com	Annunci di marketing.

Per una corretta interazione di Kaspersky Security Center Linux con i servizi esterni, tenere conto dei seguenti suggerimenti:
- Il traffico di rete non criptato deve essere consentito sulle porte 443 e 1443 dell'apparecchiatura di rete e del server proxy dell'organizzazione.
- Quando Administration Server interagisce con i server di aggiornamento Kaspersky e con i server di Kaspersky Security Network, è necessario evitare di dirottare il traffico di rete con la sostituzione del certificato (attacchi MITM).

Per scaricare gli aggiornamenti tramite il protocollo HTTP o HTTPS utilizzando l'utilità klscflag:

1. Eseguire la riga dei comandi, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella directory in cui è installato Administration Server. Il percorso di installazione predefinito è /opt/kaspersky/ksc64/sbin.

2. Se si desidera scaricare gli aggiornamenti tramite il protocollo HTTP, eseguire uno dei seguenti comandi nell'account root:

   - Nel dispositivo in cui è installato Administration Server:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - Su un punto di distribuzione;

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Se si desidera scaricare gli aggiornamenti tramite il protocollo HTTPS, eseguire uno dei seguenti comandi nell'account root:

   - Nel dispositivo in cui è installato Administration Server:

     ```
     klscflag -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - Su un punto di distribuzione;

     ```
     klscflag -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Distribuzione di Network Agent e dell'applicazione di protezione

Per gestire i dispositivi in un'organizzazione, è necessario installare Network Agent su ciascuno di essi. La distribuzione di Kaspersky Security Center Linux nei dispositivi di un'organizzazione in genere ha inizio con l'installazione di Network Agent nei dispositivi.

In Microsoft Windows XP, Network Agent potrebbe non eseguire correttamente le seguenti operazioni: scaricare gli aggiornamenti direttamente dai server Kaspersky (come punto di distribuzione) e funzionare come server proxy KSN (come punto di distribuzione).

Distribuzione iniziale

Per gestire i dispositivi in un'organizzazione, è necessario installare Network Agent su ciascuno di essi.

Per l'installazione iniziale di Network Agent su un dispositivo gestito da Linux, è possibile utilizzare i seguenti metodi:

- Collegandosi al dispositivo gestito tramite SSH ed eseguendo l'attività di installazione remota.
- Eseguendo l'installazione del pacchetto nel dispositivo gestito.

Per l'installazione iniziale di Network Agent su un dispositivo gestito da Windows, è possibile utilizzare i seguenti metodi:

- Eseguendo l'attività di installazione remota nel punto di distribuzione di Windows.
- Utilizzando il pacchetto di Windows Installer (MSI) per Network Agent, con strumenti di terze parti per l'installazione remota delle applicazioni.
- Eseguendo il programma di installazione dell'applicazione nel dispositivo gestito.
- Inviando agli utenti dei dispositivi collegamenti ai pacchetti indipendenti generati da Kaspersky Security Center Linux. I pacchetti indipendenti sono moduli eseguibili che contengono i pacchetti di distribuzione delle applicazioni selezionate, con le impostazioni predefinite.

Per l'installazione iniziale di Network Agent su un dispositivo gestito da macOS, è possibile utilizzare i seguenti metodi:

- Eseguendo l'attività di installazione remota nel punto di distribuzione macOS.
- Inviando agli utenti dei dispositivi collegamenti ai pacchetti indipendenti generati da Kaspersky Security Center Linux. I pacchetti indipendenti sono moduli eseguibili che contengono i pacchetti di distribuzione delle applicazioni selezionate, con le impostazioni predefinite.

Dopo aver installato Network Agent su un dispositivo, è possibile eseguire l'installazione remota delle applicazioni Kaspersky su tale dispositivo tramite Network Agent. Il pacchetto di distribuzione di un'applicazione da installare viene trasferito mediante i canali di comunicazione tra i Network Agent e Administration Server, insieme alle impostazioni di installazione definite dall'amministratore. Per trasferire il pacchetto di distribuzione, è possibile utilizzare nodi di distribuzione per il trasferimento, cioè punti di distribuzione, recapito multicast e così via.

Al momento della scelta di un metodo e di una strategia per la distribuzione delle applicazioni in una rete gestita, è necessario considerare diversi fattori (elenco parziale):

- Configurazione della rete dell'organizzazione.
- Numero totale di dispositivi.
- Presenza nella rete dell'organizzazione di dispositivi che non appartengono ad alcun dominio e presenza di account uniformi con diritti di amministratore su tali dispositivi.
- Capacità del canale tra l'Administration Server e i dispositivi.
- Tipo di comunicazione tra Administration Server e le subnet remote e capacità dei canali di rete in tali subnet.
- Impostazioni di sicurezza applicate sui dispositivi remoti all'inizio della distribuzione. Questi parametri consentono di stabilire la connessione remota al dispositivo gestito e di avviare l'installazione.

Configurazione dei programmi di installazione

Prima di avviare la distribuzione delle applicazioni Kaspersky in una rete, è necessario specificare le impostazioni di installazione, ovvero quelle definite durante l'installazione dell'applicazione. Durante l'installazione di Network Agent, è necessario specificare almeno un indirizzo per la connessione ad Administration Server, tuttavia possono essere richieste anche alcune impostazioni avanzate. A seconda del metodo di installazione selezionato, è possibile definire le impostazioni in diversi modi. Nel caso più semplice (installazione interattiva manuale in un dispositivo selezionato), tutte le impostazioni appropriate possono essere definite attraverso l'interfaccia utente del programma di installazione.

Questo metodo per definire le impostazioni non è appropriato per l'installazione automatica delle applicazioni in gruppi di dispositivi. In generale, l'amministratore deve specificare i valori per le impostazioni in modalità centralizzata. Tali valori possono successivamente essere utilizzati per l'installazione automatica nei dispositivi della rete selezionati.

Pacchetti di installazione

Il metodo principale per definire le impostazioni di installazione delle applicazioni è adatto per tutti i metodi di installazione, sia con gli strumenti di Kaspersky Security Center Linux che con la maggior parte strumenti di terze parti. Questo metodo consiste nella creazione di pacchetti di installazione delle applicazioni in Kaspersky Security Center Linux.

I pacchetti di installazione sono generati utilizzando i seguenti metodi:

- Automaticamente, dai pacchetti di distribuzione specificati, in base ai *descrittori* inclusi (file con estensione kud che contengono regole per l'installazione e l'analisi dei risultati e altre informazioni).
- Da un file di archivio ZIP, CAB, TAR o TAR.GZ, per applicazioni standard o supportate.

I pacchetti di installazione generati sono organizzati gerarchicamente come cartelle con sottocartelle e file. Oltre al pacchetto di distribuzione originale, un pacchetto di installazione contiene impostazioni modificabili (incluse le impostazioni del programma di installazione e le regole per elaborare casi come la necessità di riavviare il sistema operativo per completare l'installazione), nonché moduli ausiliari minori.

I valori delle impostazioni di installazione specifici per una singola applicazione supportata possono essere definiti nell'interfaccia utente di Kaspersky Security Center Web Console al momento della creazione del pacchetto di installazione. Durante l'esecuzione dell'installazione remota delle applicazioni tramite gli strumenti di Kaspersky Security Center Linux, i pacchetti di installazione vengono inviati ai dispositivi. L'esecuzione del programma di installazione di un'applicazione rende disponibili tutte le impostazioni definite dall'amministratore per tale applicazione. Quando si utilizzano strumenti di terze parti per l'installazione delle applicazioni Kaspersky, è sufficiente garantire la disponibilità dell'intero pacchetto di installazione nel dispositivo, ovvero la disponibilità del pacchetto di distribuzione e delle relative impostazioni. I pacchetti di installazione vengono creati e archiviati da Kaspersky Security Center Linux in un'apposita sottocartella della cartella condivisa.

Non specificare dettagli degli account privilegiati nei parametri dei pacchetti di installazione.

La distribuzione tramite i criteri di gruppo di Microsoft Windows non è supportata.

Subito dopo l'installazione di Kaspersky Security Center Linux, alcuni pacchetti di installazione vengono generati automaticamente: sono pronti per l'installazione e includono i pacchetti di Network Agent e i pacchetti delle applicazioni di protezione per Microsoft Windows.

Anche se è possibile impostare la chiave di licenza per un'applicazione nelle proprietà di un pacchetto di installazione, è consigliabile evitare questo metodo di distribuzione della licenza, perché è semplice ottenere l'accesso in lettura ai pacchetti di installazione. È necessario utilizzare chiavi di licenza distribuite automaticamente o le attività di installazione per le chiavi di licenza.

Informazioni sulle attività di installazione remota in Kaspersky Security Center Linux

Kaspersky Security Center Linux fornisce diversi meccanismi per l'installazione remota delle applicazioni, che sono implementati come attività di installazione remota (installazione forzata, installazione tramite copia di un'immagine del disco rigido). È possibile creare un'attività di installazione remota sia per un gruppo di amministrazione specificato che per dispositivi specifici o per una selezione di dispositivi (tali attività sono visualizzate in Kaspersky Security Center Web Console, nella cartella **Attività**). Durante la creazione di un'attività, è possibile selezionare i pacchetti di installazione (quelli di Network Agent e/o di un'altra applicazione) per l'installazione con questa attività, nonché specificare determinate impostazioni che definiscono il metodo di installazione remota. È inoltre possibile utilizzare l'Installazione remota guidata, che è basata sulla creazione di un'attività di installazione remota e sul monitoraggio dei risultati.

Le attività per i gruppi di amministrazione influiscono sia sui dispositivi inclusi in un gruppo specificato che su tutti i dispositivi in tutti i sottogruppi compresi in tale gruppo di amministrazione. Un'attività copre i dispositivi degli Administration Server secondari inclusi in un gruppo o in qualsiasi dei relativi sottogruppi se l'impostazione corrispondente è abilitata nell'attività.

Le attività per dispositivi specifici aggiornano l'elenco dei dispositivi client a ogni esecuzione, in conformità con i contenuti della selezione al momento dell'avvio dell'attività. Se una selezione include dispositivi che sono stati connessi ad Administration Server secondari, l'attività verrà eseguita anche in tali dispositivi. Per informazioni dettagliate sulle impostazioni e i metodi di installazione, vedere più avanti in questa sezione.

Per garantire la corretta esecuzione di un'attività di installazione remota nei dispositivi connessi agli Administration Server secondari, è necessario utilizzare l'attività di trasmissione per trasferire anticipatamente i pacchetti di installazione utilizzati dall'attività agli Administration Server secondari corrispondenti.

Distribuzione tramite l'acquisizione e la copia dell'immagine di un dispositivo

Se Network Agent deve essere installato in dispositivi in cui è necessario installare (o reinstallare) anche un sistema operativo e altro software, è possibile utilizzare il meccanismo di acquisizione e copia dell'immagine del dispositivo.

Per eseguire la distribuzione acquisendo e copiando un disco rigido:

1. Creare un dispositivo "di riferimento" con un sistema operativo e il software appropriato installato, incluso Network Agent e un'applicazione di protezione.

2. Acquisire l'immagine di riferimento nel dispositivo e distribuire tale immagine nei nuovi dispositivi tramite l'attività dedicata di Kaspersky Security Center Linux.

   Per acquisire e installare le immagini disco, utilizzare gli strumenti di terzi disponibili nell'organizzazione.

Copia di un'immagine disco con strumenti di terze parti

Quando si applicano strumenti di terze parti per l'acquisizione dell'immagine di un dispositivo con Network Agent installato, utilizzare uno dei seguenti metodi:

- Sul dispositivo di riferimento, interrompere il servizio Network Agent ed eseguire l'utilità klmover con l'opzione -dupfix. L'utilità klmover è inclusa nel pacchetto di installazione di Network Agent. Evitare qualsiasi successiva esecuzione del servizio Network Agent finché l'operazione di acquisizione dell'immagine non viene completata.
- Verificare che l'utilità klmover venga eseguita con l'opzione -dupfix prima (requisito obbligatorio) della prima esecuzione del servizio Network Agent nei dispositivi di destinazione, al primo avvio del sistema operativo dopo la distribuzione dell'immagine. L'utilità klmover è inclusa nel pacchetto di installazione di Network Agent.
- Utilizzare la modalità di clonazione del disco di Network Agent.

Se l'immagine del disco rigido è stata copiata in modo errato, è possibile risolvere il problema.

È inoltre possibile acquisire l'immagine di un dispositivo senza Network Agent installato. A tale scopo, eseguire la distribuzione dell'immagine nei dispositivi di destinazione, quindi distribuire Network Agent. Se si utilizza questo metodo, fornire l'accesso alla cartella di rete con i pacchetti di installazione indipendenti da un dispositivo.

Modalità di clonazione del disco di Network Agent

La clonazione del disco rigido di un dispositivo di riferimento è un popolare metodo di installazione del software nei nuovi dispositivi. Se Network Agent viene eseguito in modalità standard nel disco rigido del dispositivo di riferimento, si verifica il seguente problema:

Dopo la distribuzione dell'immagine del disco di riferimento con Network Agent nei nuovi dispositivi, questi vengono visualizzati in Kaspersky Security Center Web Console come dispositivi singoli. Questo problema si verifica perché la procedura di clonazione comporta il mantenimento nei nuovi dispositivi di dati interni identici, utilizzati da Administration Server per associare un dispositivo con il proprio record in Kaspersky Security Center Web Console.

Una specifica *modalità di clonazione del disco di Network Agent* consente di evitare i problemi associati a una visualizzazione errata dei nuovi dispositivi in Kaspersky Security Center Web Console dopo la clonazione. Utilizzare questa modalità durante la distribuzione del software (con Network Agent) nei nuovi dispositivi tramite la clonazione del disco.

Nella modalità di clonazione del disco, Network Agent continua a funzionare, ma non si connette ad Administration Server. Quando si esce dalla modalità di clonazione, Network Agent elimina i dati interni, in base ai quali Administration Server associa più dispositivi a un singolo record in Kaspersky Security Center Web Console. Al termine della clonazione dell'immagine del dispositivo di riferimento, i nuovi dispositivi sono visualizzati correttamente in Kaspersky Security Center Web Console (con singoli record).

Scenario di utilizzo della modalità di clonazione del disco di Network Agent

1. L'amministratore installa Network Agent in un dispositivo di riferimento.
2. L'amministratore verifica la connessione di Network Agent ad Administration Server utilizzando l'utilità klnagchk.
3. L'amministratore abilita la modalità di clonazione del disco di Network Agent.

4. L'amministratore installa il software e le patch nel dispositivo e lo riavvia tutte le volte che risulta necessario.
5. L'amministratore clona il disco rigido del dispositivo di riferimento in qualsiasi numero di dispositivi.
6. Ogni copia clonata deve soddisfare le seguenti condizioni:
    a. Il nome del dispositivo deve essere modificato.
    b. Il dispositivo deve essere riavviato.
    c. La modalità di clonazione del disco deve essere disabilitata.

Abilitazione e disabilitazione della modalità di clonazione del disco utilizzando l'utilità klmover

Per abilitare o disabilitare la modalità di clonazione del disco di Network Agent:

1. Eseguire l'utilità klmover nel dispositivo in cui è installato Network Agent da clonare.
   L'utilità klmover si trova nella cartella di installazione di Network Agent.
2. Per abilitare la modalità di clonazione del disco, immettere il seguente comando nel prompt dei comandi di Windows: `klmover -cloningmode 1`.
   Network Agent passa alla modalità di clonazione del disco.
3. Per richiedere lo stato corrente della modalità di clonazione del disco, immettere il seguente comando nel prompt dei comandi: `klmover -cloningmode`.
   La finestra dell'utilità indicherà se la modalità di clonazione del disco è abilitata o disabilitata.
4. Per disabilitare la modalità di clonazione del disco, immettere il seguente comando nella riga di comando dell'utilità: `klmover -cloningmode 0`.

Distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center Linux

Per eseguire la distribuzione iniziale di Network Agent o di altre applicazioni, è possibile forzare l'installazione dei pacchetti di installazione selezionati utilizzando l'attività di installazione remota di Kaspersky Security Center Linux, a condizione che ogni dispositivo disponga di uno o più account utente con diritti di amministratore locali.

L'installazione forzata può anche essere applicata se i dispositivi non sono direttamente accessibili da Administration Server, ad esempio se i dispositivi sono in rete isolata o se si trovano in una rete locale mentre Administration Server è in una rete perimetrale.

In caso di distribuzione iniziale, Network Agent non è installato. Pertanto, nelle impostazioni dell'attività di installazione remota, non è possibile selezionare la distribuzione dei file richiesti per l'installazione dell'applicazione utilizzando Network Agent. È possibile scegliere di distribuire i file solo utilizzando le risorse del sistema operativo tramite Administration Server o i punti di distribuzione.

Il servizio Administration Server deve essere eseguito con un account con privilegi di amministratore nei dispositivi di destinazione. In alternativa, è possibile specificare un account che ha accesso alla condivisione admin$ nelle impostazioni dell'attività di installazione remota.

Per impostazione predefinita, l'attività di installazione remota viene applicata ai dispositivi utilizzando le credenziali dell'account con cui è in esecuzione Administration Server. È importante chiarire che questo è l'account utilizzato per accedere alla condivisione admin$, anziché l'account con cui viene eseguita l'attività di installazione remota. L'installazione viene eseguita con l'account LocalSystem.

È possibile specificare i dispositivi di destinazione esplicitamente (con un elenco), selezionando il gruppo di amministrazione di Kaspersky Security Center Linux a cui appartengono o creando una selezione di dispositivi in base a un criterio specifico. L'ora di inizio dell'installazione è definita dalla pianificazione dell'attività. Se l'impostazione **Esegui attività non effettuate** è abilitata nelle proprietà dell'attività, l'attività può essere eseguita subito dopo l'accensione dei dispositivi di destinazione o quando vengono spostati nel gruppo di amministrazione di destinazione.

L'installazione forzata consiste nella distribuzione dei pacchetti di installazione ai dispositivi di destinazione, nella successiva copia dei file nella risorsa admin$ in ciascuno dei dispositivi di destinazione e nella registrazione remota dei servizi di supporto in tali dispositivi. L'invio dei pacchetti di installazione ai dispositivi di destinazione viene eseguito tramite una funzionalità di Kaspersky Security Center Linux che garantisce l'interazione di rete. In questo caso, devono essere soddisfatte le seguenti condizioni:

- I dispositivi di destinazione sono accessibili dal lato di Administration Server o dal lato del punto di distribuzione.
- La risoluzione dei nomi per i dispositivi di destinazione funziona correttamente nella rete.
- Le condivisioni amministrative (admin$) rimangono abilitate nei dispositivi di destinazione.
- I seguenti servizi di sistema sono in esecuzione nei dispositivi di destinazione:
  - Server (LanmanServer)

    Per impostazione predefinita, questo servizio è in esecuzione.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- La porta TCP 445 è aperta nei dispositivi di destinazione per abilitare l'accesso remoto tramite Windows Management Instrumentation.

  TCP 139, UDP 137 e UDP 138 vengono utilizzati dai protocolli precedenti e non sono più necessari per le applicazioni correnti.

  Le porte di accesso dinamiche in uscita devono essere consentite nel firewall per le connessioni da Administration Server e dai punti di distribuzione ai dispositivi di destinazione.
- Le impostazioni di protezione del criterio di dominio di Active Directory possono fornire il funzionamento del protocollo NTLM durante la distribuzione di Network Agent.
- Nei dispositivi di destinazione che eseguono Microsoft Windows XP, la modalità Simple File Sharing è disabilitata.
- Nei dispositivi di destinazione, il modello di protezione e condivisione dell'accesso è impostato su *Classico: gli utenti locali eseguono l'autenticazione come se stessi*. Non può in alcun modo essere *Solo Guest: gli utenti locali si autenticano come Guest*.

- I dispositivi di destinazione sono utenti del dominio o vengono creati anticipatamente account uniformi con diritti di amministratore nei dispositivi di destinazione.

Per distribuire correttamente Network Agent o altre applicazioni in un dispositivo che non fa parte di un dominio Active Directory di Windows Server 2003 o versione successiva, è necessario disabilitare Controllo dell'account utente remoto in tale dispositivo. Controllo dell'account utente remoto è uno dei motivi che impedisce agli account amministrativi locali di accedere ad admin$, necessario per la distribuzione forzata di Network Agent o di altre applicazioni. La disabilitazione di Controllo dell'account utente remoto non influisce su Controllo dell'account utente locale.

Durante l'installazione in nuovi dispositivi che non sono stati ancora assegnati ad alcun gruppo di amministrazione di Kaspersky Security Center Linux, è possibile aprire le proprietà dell'attività di installazione remota e specificare il gruppo di amministrazione in cui spostare i dispositivi dopo l'installazione di Network Agent.

Al momento della creazione di un'attività di gruppo, tenere presente che ogni attività di gruppo influisce su tutti i dispositivi in tutti i gruppi nidificati all'interno un gruppo selezionato. È pertanto necessario evitare di duplicare le attività di installazione nei sottogruppi.

Un modo semplificato per creare attività per l'installazione forzata delle applicazioni è l'installazione automatica. A tale scopo, è necessario aprire le proprietà del gruppo di amministrazione, aprire l'elenco dei pacchetti di installazione e selezionare quelli da installare nei dispositivi di questo gruppo. I pacchetti di installazione selezionati saranno installati automaticamente in tutti i dispositivi di questo gruppo e di tutti i relativi sottogruppi. L'intervallo di tempo richiesto per l'installazione dei pacchetti dipende dalla velocità effettiva della rete e dal numero totale di dispositivi in rete.

Per ridurre il carico su Administration Server durante la distribuzione dei pacchetti di installazione ai dispositivi di destinazione, è possibile selezionare l'installazione tramite i punti di distribuzione nell'attività di installazione. Tenere presente che questo metodo di installazione comporta un carico significativo per i dispositivi che operano come punti di distribuzione. Pertanto, si consiglia di selezionare i dispositivi che soddisfano i requisiti per i punti di distribuzione. Se si utilizzano punti di distribuzione, è necessario assicurarsi che siano presenti in ciascuna delle subnet isolate che ospitano i dispositivi di destinazione.

L'utilizzo dei punti di distribuzione come centri di installazione locali può anche essere utile durante l'installazione nei dispositivi in subnet che comunicano con Administration Server tramite un canale con una capacità limitata, mentre è disponibile un canale con una maggiore capacità tra i dispositivi nella stessa subnet.

Lo spazio libero su disco nella partizione con la cartella /var/opt/kaspersky/KSC_Backups* deve superare, di diverse volte, le dimensioni totali dei pacchetti di distribuzione delle applicazioni installate.

Esecuzione di pacchetti indipendenti creati tramite Kaspersky Security Center Linux

I metodi descritti in precedenza per la distribuzione iniziale di Network Agent e delle altre applicazioni non possono essere sempre implementati perché non è possibile soddisfare tutte le condizioni applicabili. In tali casi, è possibile creare un comune file eseguibile denominato *pacchetto di installazione indipendente* tramite Kaspersky Security Center Linux, utilizzando i pacchetti di installazione con le impostazioni di installazione appropriate che sono stati preparati dall'amministratore. Il pacchetto di installazione indipendente è archiviato nella cartella condivisa di Kaspersky Security Center Linux.

È possibile utilizzare Kaspersky Security Center Linux per inviare agli utenti selezionati un messaggio e-mail che contiene un collegamento a questo file nella cartella condivisa, richiedendo loro di eseguire il file (in modalità interattiva o con l'opzione "-s" per l'installazione automatica). È possibile allegare il pacchetto di installazione indipendente a un messaggio e-mail e quindi inviarlo agli utenti dei dispositivi che non hanno accesso alla cartella condivisa di Kaspersky Security Center Linux. L'amministratore può anche copiare il pacchetto indipendente in un'unità rimovibile, trasferirlo in un dispositivo appropriato e quindi eseguirlo in un secondo momento.

È possibile creare un pacchetto indipendente da un pacchetto di Network Agent, un pacchetto di un'altra applicazione (ad esempio, l'applicazione di protezione) o entrambi. Se il pacchetto indipendente è stato creato da Network Agent e un'altra applicazione, l'installazione inizia da Network Agent.

Durante la creazione di un pacchetto indipendente con Network Agent, è possibile specificare il gruppo di amministrazione nel quale verranno automaticamente spostati i nuovi dispositivi (quelli che non sono stati allocati ad alcun gruppo di amministrazione) al termine dell'installazione di Network Agent.

I pacchetti indipendenti possono essere eseguiti in modalità interattiva (per impostazione predefinita), visualizzando il risultato dell'installazione delle applicazioni che contengono, o possono essere eseguiti in modalità automatica (con l'opzione "-s"). La modalità automatica può essere utilizzata per l'installazione tramite script, ad esempio script configurati per l'esecuzione dopo la distribuzione dell'immagine di un sistema operativo. Il risultato dell'installazione in modalità automatica è determinato dal codice restituito del processo.

Installazione remota delle applicazioni nei dispositivi in cui è installato Network Agent

Se un Network Agent connesso all'Administration Server primario (o a uno dei relativi Server secondari) è installato in un dispositivo, è possibile eseguire l'upgrade di Network Agent in tale dispositivo, nonché installare, aggiornare o rimuovere qualsiasi applicazione supportata tramite Network Agent.

È possibile abilitare l'opzione **Utilizzando Network Agent** nelle proprietà dell'attività di installazione remota.

Se questa opzione è selezionata, i pacchetti di installazione con le impostazioni di installazione definite dall'amministratore saranno trasferiti ai dispositivi di destinazione tramite i canali di comunicazione tra Network Agent e Administration Server.

Per ottimizzare il carico su Administration Server e ridurre al minimo il traffico tra Administration Server e i dispositivi, è consigliabile assegnare punti di distribuzione in ogni rete remota o in ogni dominio di trasmissione (vedere le sezioni "Informazioni sui punti di distribuzione" e "Creazione di una struttura di gruppi di amministrazione e assegnazione dei punti di distribuzione". In questo caso, i pacchetti di installazione e le impostazioni del programma di installazione sono distribuiti dall'Administration Server ai dispositivi di destinazione tramite i punti di distribuzione.

È inoltre possibile utilizzare i punti di distribuzione per l'invio (multicast) dei pacchetti di installazione, che consente di ridurre considerevolmente il traffico di rete durante la distribuzione delle applicazioni.

Durante il trasferimento dei pacchetti di installazione ai dispositivi di destinazione tramite i canali di comunicazione tra i Network Agent e l'Administration Server, tutti i pacchetti di installazione che sono stati preparati per il trasferimento saranno anche memorizzati nella cache nella cartella /var/opt/kaspersky/klnagent_srv/1093/.working/. Quando si utilizzano diversi pacchetti di installazione di grandi dimensioni, di vari tipi e che coinvolgono numerosi punti di distribuzione, le dimensioni di questa cartella possono aumentare notevolmente.

I file non possono essere eliminati manualmente della cartella FTServer. Quando i pacchetti di installazione originali vengono eliminati, i dati corrispondenti sono eliminati automaticamente della cartella FTServer.

I dati ricevuti dai punti di distribuzione vengono salvati nella cartella /var/opt/kaspersky/klnagent_srv/1103/.

I file non possono essere eliminati manualmente della cartella $FTClTmp. Al termine delle attività che utilizzano i dati in questa cartella, i contenuti della cartella saranno eliminati automaticamente.

Poiché i pacchetti di installazione sono distribuiti tramite i canali di comunicazione tra Administration Server e i Network Agent da un archivio intermedio in un formato ottimizzato per i trasferimenti in rete, non sono consentite modifiche ai pacchetti di installazione archiviati nella cartella originale di ogni pacchetto di installazione. Tali modifiche non saranno registrate automaticamente da Administration Server. Se è necessario modificare manualmente i file dei pacchetti di installazione (sebbene sia consigliabile evitare questo scenario), è necessario modificare qualsiasi impostazione di un pacchetto di installazione in Kaspersky Security Center Web Console. La modifica delle impostazioni di un pacchetto di installazione in Kaspersky Security Center Web Console fa sì che Administration Server aggiorni l'immagine del pacchetto nella cache che è stato preparato per il trasferimento nei dispositivi di destinazione.

Il server invia richieste echo ICMP (lo stesso del comando ping) al dispositivo di destinazione durante l'installazione remota.

Gestione dei riavvii dei dispositivi nell'attività di installazione remota

I dispositivi spesso richiedono un riavvio per completare l'installazione remota delle applicazioni (in particolare in Windows).

Se si utilizza l'attività Installazione remota di Kaspersky Security Center Linux, nella Creazione guidata nuova attività o nella finestra delle proprietà dell'attività che è stata creata (sezione **Riavvio del sistema operativo**), è possibile selezionare l'azione da eseguire quando il dispositivo Windows richiede un riavvio:

- **Non riavviare il dispositivo**. In questo caso, non sarà eseguito alcun riavvio automatico. Per completare l'installazione, è necessario riavviare il dispositivo (ad esempio, manualmente o tramite l'attività di gestione del dispositivo). Le informazioni sul riavvio richiesto saranno salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività di installazione nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**. In questo caso, il dispositivo viene sempre riavviato automaticamente quando è richiesto un riavvio per il completamento dell'installazione. Questa opzione è utile per le attività di installazione nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**. In questo caso, sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). L'opzione **Richiedi l'intervento dell'utente** è la più adatta per le workstation, in cui gli utenti devono avere la possibilità di selezionare l'orario che preferiscono per un riavvio del sistema.

Aggiornamento dei database in un pacchetto di installazione di un'applicazione di protezione

Prima di avviare la distribuzione della protezione, è necessario tenere presente che è possibile aggiornare i database anti-virus (inclusi i moduli delle patch automatiche) forniti con il pacchetto di distribuzione dell'applicazione di protezione. È consigliabile aggiornare i database nel pacchetto di installazione dell'applicazione prima di avviare la distribuzione (ad esempio, utilizzando il comando corrispondente nel menu di scelta rapida di un pacchetto di installazione selezionato). In tal modo, è possibile ridurre il numero di riavvii richiesti per il completamento della distribuzione della protezione nei dispositivi di destinazione.

Monitoraggio della distribuzione

Per monitorare la distribuzione di Kaspersky Security Center Linux e assicurarsi che un'applicazione di protezione e Network Agent siano installati nei dispositivi gestiti, utilizzare la funzionalità di monitoraggio e generazione dei rapporti:

- Utilizzare il widget di distribuzione del dashboard per monitorare la distribuzione in tempo reale.
- Utilizzare i rapporti per ottenere informazioni dettagliate.

Configurazione dei programmi di installazione

Questa sezione fornisce informazioni sui file dei programmi di installazione di Kaspersky Security Center Linux e sulle impostazioni di installazione, oltre a raccomandazioni su come installare Administration Server e Network Agent in modalità automatica.

Informazioni generali

I programmi di installazione dei componenti di Kaspersky Security Center Linux per dispositivi Windows sono basati sulla tecnologia Windows Installer. L'elemento fondamentale di un programma di installazione è un pacchetto MSI. Questo formato dei pacchetti consente di sfruttare tutti i vantaggi offerti da Windows Installer: la scalabilità, la disponibilità di un sistema di applicazione delle patch, il sistema di trasformazione, l'installazione centralizzata tramite soluzioni di terze parti e la registrazione trasparente con il sistema operativo.

Parametri di installazione di Administration Server

La tabella seguente descrive le proprietà che è possibile configurare durante l'installazione di Kaspersky Security Center Linux in modalità automatica.

Parametri dell'installazione di Administration Server in modalità automatica

Nome della variabile	Richiesto	Descrizione	Valori possibili
EULA_ACCEPTED	Sì	Conferma che l'utente ha compreso e accettato i termini del Contratto di licenza con l'utente finale.	1
PP_ACCEPTED	Sì	Conferma che l'utente ha compreso e accettato i termini dell'Informativa sulla privacy.	1
KLSRV_UNATT_SERVERADDRESS	Sì	Il nome DNS o l'indirizzo IP statico di Administration Server.	Nome DNS o indirizzo IP
KLSRV_UNATT_PORT_SRV	No	Il numero di porta di Administration Server.	Numero di porta

		Facoltativamente, il valore predefinito è 14000.	
KLSRV_UNATT_PORT_SRV_SSL	No	Il numero di porta SSL di Administration Server. Facoltativamente, il valore predefinito è 13000.	Numero di porta
KLSRV_UNATT_PORT_KLOAPI	No	Il numero di porta KLOAPI di Administration Server. Facoltativamente, il valore predefinito è 13299.	Numero di porta
KLSRV_UNATT_PORT_GUI	No	Il numero di porta GUI di Administration Server. Facoltativamente, il valore predefinito è 13291.	Numero di porta
KLSRV_UNATT_NETRANGETYPE	No	Il numero approssimativo di dispositivi che si intende gestire. Facoltativamente, il valore predefinito è 1.	1 per 1-100 dispositivi in rete. 2 per 101-1000 dispositivi in rete. 3 per oltre 1000 dispositivi in rete.
KLSRV_UNATT_DBMS_TYPE	Sì	Il tipo di sistema di gestione dei database: MySQL (MariaDB) o Postgres.	mysql o postgres
KLSRV_UNATT_DBMS_INSTANCE	Sì	L'indirizzo IP del server di database.	Indirizzo IP
KLSRV_UNATT_DBMS_PORT	Sì	La porta del server di database. Il valore predefinito per MySQL (MariaDB) è 3306; il valore predefinito per Postgres è 5432.	3306 o 5432
KLSRV_UNATT_DB_NAME	Sì	Il nome del database.	kav
KLSRV_UNATT_DBMS_LOGIN	Sì	Il nome utente di un utente che ha accesso al database.	
KLSRV_UNATT_DBMS_PASSWORD	Sì	La password di un utente che ha accesso al database.	
KLSRV_UNATT_KLADMINSGROUP	Sì	Il nome del gruppo di protezione per i servizi.	kladmins
KLSRV_UNATT_KLSRVUSER	Sì	Il nome dell'account per avviare il servizio Administration Server. L'account deve essere un membro del gruppo di sicurezza specificato nella variabile KLSRV_UNATT_KLADMINSGROUP.	ksc
KLSRV_UNATT_KLSVCUSER	Sì	Il nome dell'account per avviare altri servizi. L'account deve essere un membro del gruppo di sicurezza specificato nella variabile KLSRV_UNATT_KLADMINSGROUP.	ksc
Se Administration Server deve essere distribuito come cluster di failover Kaspersky Security Center Linux, il file di risposte deve includere le seguenti variabili aggiuntive:			
KLFOC_UNATT_NODE	Sì	Il numero del nodo (1 o 2).	1 o 2
KLFOC_UNATT_STATE_SHARE_MOUNT_PATH	Sì	Il punto di montaggio della condivisione degli stati.	
KLFOC_UNATT_DATA_SHARE_MOUNT_PATH	Sì	Il punto di montaggio della condivisione dei dati.	
KLFOC_UNATT_CONN_MODE	Sì	La modalità di connettività del cluster di failover.	VirtualAdapter o ExternalLoadBalancer
Nel caso in cui la variabile KLFOC_UNATT_CONN_MODE abbia un valore VirtualAdapter, il file di risposte deve includere le seguenti variabili aggiuntive:			
KLFOC_UNATT_CONN_MODE_VA_NAME	Sì	Il nome della scheda di rete virtuale.	
KLFOC_UNATT_CONN_MODE_VA_IPV4	Una di queste variabili è obbligatoria	L'indirizzo IP della scheda di rete virtuale.	Indirizzo IP
KLFOC_UNATT_CONN_MODE_VA_IPV6		L'indirizzo IPv6 della scheda di rete virtuale.	Indirizzo IPv6

Parametri di installazione di Network Agent

Nella tabella seguente sono descritte le proprietà MSI che è possibile configurare durante l'installazione di Network Agent. Tutti i parametri sono facoltativi, ad eccezione di EULA e SERVERADDRESS.

Parametri dell'installazione di Network Agent in modalità automatica

Proprietà MSI	Descrizione	Valori disponibili
EULA	Accettazione del Contratto di licenza	• 1 - Confermo di aver letto, compreso e accettato i termini e le condizioni del presente Contratto di licenza con l'utente finale. • 0—Non accetto i termini del Contratto di licenza (l'installazione non viene eseguita). • Nessun valore—Non accetto i termini del Contratto di licenza (l'installazione non viene eseguita).
DONT_USE_ANSWER_FILE	Leggere le impostazioni di installazione dal file di risposta	• 1—Non utilizzare. • Altri valori o nessun valore—Lettura.
INSTALLDIR	Percorso della cartella di installazione di Network Agent	Valore stringa.
SERVERADDRESS	Indirizzo di Administration Server (obbligatorio)	Valore stringa.
SERVERPORT	Numero di porta per la connessione ad Administration Server	Valore numerico.
SERVERSSLPORT	Numero di porta per la connessione criptata ad Administration Server tramite il protocollo SSL	Valore numerico.
USESSL	Specifica se utilizzare connessione SSL	• 1 - Utilizzare. • Altri valori o nessun valore - Non utilizzare.
OPENUDPPORT	Specifica se aprire una porta UDP	• 1 - Aprire. • Altri valori o nessun valore - Non aprire.
UDPPORT	Numero di porta UDP	Valore numerico.
USEPROXY	Specifica se utilizzare un server proxy: Per motivi di compatibilità, non è consigliabile specificare le impostazioni di connessione proxy nelle impostazioni del pacchetto di installazione di Network Agent.	• 1 - Utilizzare. • Altri valori o nessun valore - Non utilizzare.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Indirizzo del proxy e numero di porta per la connessione al server proxy	Valore stringa.
PROXYLOGIN	Account per la connessione a un server proxy	Valore stringa.
PROXYPASSWORD	Password dell'account per la connessione al server proxy (non specificare i dettagli degli account con privilegi nei parametri dei pacchetti di installazione.)	Valore stringa.
GATEWAYMODE	Modalità di utilizzo del gateway di connessione	• 0 - Non utilizzare il gateway di connessione. • 1 - Utilizza questo Network Agent come gateway di connessione. • 2 - Connetti ad Administration Server utilizzando il gateway di connessione.
GATEWAYADDRESS	Indirizzo gateway connessione	Valore stringa.
CERTSELECTION	Metodo di ricezione di un certificato	• GetOnFirstConnection - Ricevere un certificato da Administration Server.

		• GetExistent - Selezionare un certificato esistente. Se questa opzione è selezionata, è necessario specificare la proprietà CERTFILE.
CERTFILE	Percorso del file di certificato	Valore stringa.
VMVDI	Abilitare la modalità dinamica per Virtual Desktop Infrastructure (VDI)	• 1 - Abilitare. • 0 - Non abilitare. • Nessun valore - Non abilitare.
LAUNCHPROGRAM	Specifica se avviare il servizio Network Agent dopo l'installazione. Il parametro viene ignorato se VMVDI=1	• 1 - Avviare. • Altri valori o nessun valore - Non avviare.
NAGENTTAGS	Tag per Network Agent (ha la priorità sul tag assegnato nel file di risposta)	Valore stringa.

Infrastruttura virtuale

Kaspersky Security Center Linux supporta l'utilizzo di macchine virtuali. È possibile installare Network Agent e l'applicazione di protezione in ogni macchina virtuale, nonché proteggere le macchine virtuali a livello di hypervisor. Nel primo caso è possibile utilizzare un'applicazione di protezione standard o Kaspersky Security for Virtualization Light Agent per proteggere le macchine virtuali. Nel secondo caso è possibile utilizzare Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center Linux supporta i rollback delle macchine virtuali allo stato precedente.

Suggerimenti per la riduzione del carico sulle macchine virtuali

Durante l'installazione di Network Agent in una macchina virtuale, è consigliabile valutare se disabilitare alcune funzionalità di Kaspersky Security Center Linux che risultano di scarsa utilità per le macchine virtuali.

Quando si installa Network Agent in una macchina virtuale o in un modello utilizzato per la generazione di macchine virtuali, è consigliabile eseguire le seguenti azioni:

- Se si esegue un'installazione remota, nella finestra delle proprietà del pacchetto di installazione di Network Agent, nella sezione **Avanzate** selezionare l'opzione **Ottimizza le impostazioni per VDI**.
- Se si esegue un'installazione interattiva tramite una procedura guidata, nella finestra della procedura guidata selezionare l'opzione **Ottimizza le impostazioni di Network Agent per l'infrastruttura virtuale**.

La selezione di queste opzioni modifica le impostazioni di Network Agent in modo da mantenere disabilitate le seguenti funzionalità per impostazione predefinita (prima dell'applicazione di un criterio):

- Recupero delle informazioni sul software installato
- Recupero delle informazioni sull'hardware
- Recupero delle informazioni sulle vulnerabilità rilevate
- Recupero delle informazioni sugli aggiornamenti richiesti

In genere, queste funzionalità non sono necessarie nelle macchine virtuali perché utilizzano software uniforme e hardware virtuale.

La disabilitazione delle funzionalità è reversibile. Se è richiesta una delle funzionalità disabilitate, è possibile abilitarla tramite il criterio di Network Agent o mediante le impostazioni locali di Network Agent. Le impostazioni locali di Network Agent sono disponibili tramite il menu di scelta rapida del dispositivo appropriato in Kaspersky Security Center Web Console.

Supporto delle macchine virtuali dinamiche

Kaspersky Security Center Linux supporta le macchine virtuali dinamiche. Se nella rete dell'organizzazione è stata distribuita un'infrastruttura virtuale, in alcuni casi è possibile utilizzare macchine virtuali (temporanee) dinamiche. Le macchine virtuali dinamiche vengono create con nomi univoci in base a un modello che è stato preparato dall'amministratore. L'utente lavora su una macchina virtuale per un certo periodo e, dopo lo spegnimento, questa macchina virtuale sarà rimossa dall'infrastruttura virtuale. Se Kaspersky Security Center Linux è stato distribuito nella rete dell'organizzazione, una macchina virtuale con Network Agent installato verrà aggiunta al database di Administration Server. Dopo lo spegnimento di una macchina virtuale, anche la voce corrispondente deve essere rimossa dal database di Administration Server.

Per rendere disponibile la funzionalità di rimozione automatica delle voci nelle macchine virtuali, durante l'installazione di Network Agent in un modello per le macchine virtuali dinamiche, selezionare l'opzione **Abilita modalità dinamica per VDI**:

- Per l'installazione remota - Nella finestra delle proprietà del pacchetto di installazione di Network Agent (sezione **Avanzate**)
- Per l'installazione interattiva - Nell'Installazione guidata di Network Agent

Evitare di selezionare l'opzione **Abilita modalità dinamica per VDI** durante l'installazione di Network Agent nei dispositivi fisici.

Se si desidera archiviare gli eventi generati dalle macchine virtuali dinamiche in Administration Server per un certo periodo dopo la rimozione delle macchine virtuali, nella finestra delle proprietà di Administration Server, nella sezione **Archivio eventi**, selezionare l'opzione **Archivia eventi dopo l'eliminazione dei dispositivi** e specificare il periodo di archiviazione massimo degli eventi (in giorni).

Supporto della copia delle macchine virtuali

La copia di una macchina virtuale con Network Agent installato o la creazione di una macchina virtuale da un modello con Network Agent installato sono identiche alla distribuzione dei Network Agent tramite l'acquisizione e la copia di un'immagine del disco rigido. In generale, durante la copia delle macchine virtuali è necessario eseguire le stesse azioni previste durante la distribuzione di Network Agent tramite la copia un'immagine del disco.

Tuttavia, nei due casi descritti di seguito viene illustrato Network Agent, che rileva automaticamente la copia. Per i motivi indicati in precedenza, non è necessario eseguire le operazioni sofisticate descritte in "Distribuzione tramite l'acquisizione e la copia dell'immagine del disco rigido di un dispositivo":

- L'opzione **Abilita modalità dinamica per VDI** era selezionata durante l'installazione di Network Agent: dopo ogni riavvio del sistema operativo, questa macchina virtuale sarà riconosciuta come un nuovo dispositivo, indipendentemente dal fatto che sia stata copiata.

- È in uso uno dei seguenti hypervisor: VMware™, HyperV® o Xen®: Network Agent rileva la copia della macchina virtuale in base agli ID modificati dell'hardware virtuale.

L'analisi delle modifiche nell'hardware virtuale non è assolutamente affidabile. Prima di applicare questo metodo su larga scala, è necessario testarlo su un piccolo gruppo di macchine virtuali per la versione dell'hypervisor attualmente in uso nell'organizzazione.

Supporto del rollback del file system per i dispositivi con Network Agent

Kaspersky Security Center Linux è un'applicazione distribuita. Il rollback del file system uno stato precedente in un dispositivo con Network Agent installato determinerà la mancata sincronizzazione dei dati e impedirà il corretto funzionamento di Kaspersky Security Center Linux.

È possibile eseguire il rollback del file system (o di una sua parte) nei seguenti casi:

- Durante la copia di un'immagine del disco rigido.
- Durante il ripristino di uno stato della macchina virtuale tramite l'infrastruttura virtuale.
- Durante il ripristino dei dati da una copia di backup o da un punto di ripristino.

Gli scenari in cui software di terze parti nei dispositivi con Network Agent installato influisce sulla directory /var/opt/kaspersky/klnagent sono solo scenari critici per Kaspersky Security Center Linux. Pertanto, è necessario escludere sempre questa cartella dalla procedura di ripristino, se possibile.

Dal momento che le regole per l'ambiente di lavoro di alcune organizzazioni consentono i rollback del file system nei dispositivi, il supporto per il rollback del file system nei dispositivi con Network Agent installato è stato aggiunto a Kaspersky Security Center Linux a partire dalla versione 10 Maintenance Release 1 (Administration Server e i Network Agent devono essere della versione 10 Maintenance Release 1 o successiva). Quando sono rilevati, tali dispositivi vengono riconnessi automaticamente all'Administration Server con una cancellazione completa dei dati e una sincronizzazione completa.

Per impostazione predefinita, il supporto per il rilevamento del rollback del file system è abilitato in Kaspersky Security Center Linux.

Per quanto possibile, evitare di eseguire il rollback della directory /var/opt/kaspersky/klnagent nei dispositivi con Network Agent installato, perché la risincronizzazione completa dei dati richiede una notevole quantità di risorse.

Non è assolutamente consentito un rollback dello stato del sistema in un dispositivo con Administration Server installato, né un rollback del database utilizzato da Administration Server.

È possibile ripristinare uno stato di Administration Server da una copia di backup solo con l'utilità klbackup standard.

Installazione locale delle applicazioni

In questa sezione viene descritta una procedura di installazione per le applicazioni che possono essere installate solo nei dispositivi in locale.

Per eseguire l'installazione locale delle applicazioni in un dispositivo client specifico, è necessario disporre di diritti di amministratore per il dispositivo.

Per installare le applicazioni in locale in un dispositivo client specifico:

1. Installare Network Agent nel dispositivo client e configurare la connessione tra il dispositivo client e Administration Server.

2. Installare le applicazioni richieste nel dispositivo, come descritto nei manuali delle applicazioni.

3. Installare un plug-in di gestione per ognuna delle applicazioni installate nella workstation dell'amministratore.

Kaspersky Security Center Linux supporta inoltre l'opzione per l'installazione locale delle applicazioni utilizzando un pacchetto di installazione indipendente. Kaspersky Security Center Linux non supporta l'installazione di tutte le applicazioni Kaspersky.

Installazione di Network Agent per Linux in modalità interattiva

Questo articolo descrive come installare Network Agent nei dispositivi Linux in modalità interattiva, specificando passo dopo passo i parametri di installazione. In alternativa, è possibile utilizzare un file di risposte: un file di testo contenente un set personalizzato di parametri di installazione: variabili e rispettivi valori. L'uso di questo file di risposte consente di eseguire un'installazione in modalità automatica, ovvero senza la partecipazione dell'utente.

Per installare Network Agent in modalità interattiva:

1. Eseguire l'installazione di Network Agent. A seconda della distribuzione Linux, eseguire uno dei seguenti comandi:

   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 32 bit:

     ```
     # yum -i klnagent-<numero build>.i386.rpm
     ```

   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 64 bit:

     ```
     # yum -i klnagent64-<numero build>.x86_64.rpm
     ```

   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 64 bit per l'architettura Arm:

     ```
     # yum -i klnagent64-<numero build>.aarch64.rpm
     ```

   - Per installare Network Agent da un pacchetto DEB in un sistema operativo a 32 bit:

     ```
     # apt install ./klnagent_<numero build>_i386.deb
     ```

   - Per installare Network Agent da un pacchetto DEB in un sistema operativo a 64 bit:

     ```
     # apt install ./klnagent64_<numero build>_amd64.deb
     ```

   - Per installare Network Agent da un pacchetto DEB in un sistema operativo a 64 bit per l'architettura Arm:

     ```
     # apt install ./klnagent64_<numero build>_arm64.deb
     ```

2. Eseguire la configurazione di Network Agent:

   ```
   # /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Leggere il Contratto di licenza con l'utente finale (EULA). Il testo viene visualizzato nella finestra della riga di comando. Premere la barra spaziatrice per visualizzare il segmento di testo successivo. Quando richiesto

inserire uno dei seguenti valori:

- Immettere `y` se i termini del Contratto di licenza con l'utente finale sono stati compresi e accettati.
- Immettere `n` se non si accettano i termini del Contratto di licenza con l'utente finale. Per utilizzare Network Agent, è necessario accettare i termini del Contratto di licenza con l'utente finale.
- Immettere `r` per mostrare nuovamente il Contratto di licenza con l'utente finale.

4. Immettere l'indirizzo IP o il nome DNS di Administration Server.
5. Immettere il numero di porta di Administration Server. Per impostazione predefinita, viene utilizzata la porta 14000.
6. Immettere il numero di porta SSL di Administration Server. Per impostazione predefinita, viene utilizzata la porta 13000.
7. Immettere `y` se si desidera utilizzare il criptaggio SSL per il traffico tra Network Agent e Administration Server. In caso contrario, immettere `n`.
8. Selezionare una delle seguenti opzioni per configurare Network Agent:
   - `[1]`: non configurare un gateway di connessione.

     Il dispositivo non fungerà da gateway di connessione e non si connetterà ad Administration Server tramite un gateway di connessione.
   - `[2]`: non utilizzare un gateway di connessione.

     Il dispositivo non si connetterà ad Administration Server tramite un gateway di connessione.
   - `[3]`: eseguire la connessione al server utilizzando un gateway di connessione.

     Il dispositivo si connetterà ad Administration Server tramite un gateway di connessione.
   - `[4]`: utilizzare come gateway di connessione.

     Il dispositivo fungerà da gateway di connessione.

Network Agent viene installato in un dispositivo Linux.

Installazione di Network Agent per Windows in modalità interattiva

Per installare Network Agent in locale in un dispositivo:

1. Nel dispositivo, eseguire il file ksc_<numero versione>.<numero build>_full_<lingua localizzazione>.exe dal pacchetto di distribuzione scaricato da internet.

   Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da installare.
2. Nella finestra di selezione dell'applicazione fare clic sul collegamento **Installa solo Kaspersky Security Center 15 Network Agent** per avviare l'Installazione guidata di Network Agent. Seguire le istruzioni della procedura guidata.

   Durante l'esecuzione dell'Installazione guidata, è possibile specificare le impostazioni avanzate di Network Agent (vedere di seguito).

3. Se si desidera utilizzare il dispositivo come gateway di connessione per uno specifico gruppo di amministrazione, nella finestra **Gateway di connessione** dell'Installazione guidata selezionare **Use Network Agent as connection gateway in DMZ**.

4. Per configurare Network Agent durante l'installazione in una macchina virtuale:

   a. Se si prevede di creare macchine virtuali dinamiche dall'immagine della macchina virtuale, abilitare la modalità dinamica di Network Agent per Virtual Desktop Infrastructure (VDI). A tale scopo, nella finestra **Impostazioni avanzate** dell'Installazione guidata selezionare l'opzione **Abilita modalità dinamica per VDI**.

   Ignorare questo passaggio se non si prevede di creare macchine virtuali dinamiche dall'immagine della macchina virtuale.

   b. Ottimizzare il funzionamento di Network Agent per VDI. A tale scopo, nella finestra **Impostazioni avanzate** dell'Installazione guidata, selezionare l'opzione **Ottimizza le impostazioni per VDI**.

   Verrà disabilitata la scansione dei file eseguibili per rilevare la presenza di vulnerabilità all'avvio del dispositivo. Inoltre, verrà disabilitato l'invio di informazioni sui seguenti oggetti ad Administration Server:

   - Registro hardware
   - Applicazioni installate nel dispositivo
   - Aggiornamenti di Microsoft Windows da installare nel dispositivo client locale
   - Vulnerabilità del software rilevate nel dispositivo client locale

   Inoltre, sarà possibile abilitare l'invio di queste informazioni nelle proprietà di Network Agent o nelle impostazioni del criterio di Network Agent.

Al termine dell'Installazione guidata, Network Agent viene installato nel dispositivo.

È possibile visualizzare le proprietà del servizio Network Agent; è inoltre possibile avviare, arrestare e monitorare l'esecuzione di Network Agent utilizzando gli strumenti standard di Microsoft Windows: Gestione computer\Servizi.

Installazione di Network Agent for Windows in modalità automatica

Network Agent può essere installato in modalità automatica, ovvero senza l'input dei parametri di installazione. L'installazione automatica utilizza un pacchetto di installazione di Windows (MSI) per Network Agent. Il file MSI è disponibile nel pacchetto di distribuzione di Kaspersky Security Center Linux, nella cartella Packages\NetAgent\exec.

L'installazione di Network Agent dal pacchetto MSI è possibile solo in modalità automatica, l'installazione interattiva dal pacchetto MSI non è supportata.

Per installare Network Agent in un dispositivo locale in modalità automatica:

1. Leggere il Contratto di licenza con l'utente finale. Utilizzare il comando di seguito solo se sono stati compresi e accettati i termini del Contratto di licenza con l'utente finale.

2. Eseguire il comando

```
msiexec /i "Kaspersky Network Agent.msi" /qn <parametri_installazione>
```

dove `parametri_installazione` è un elenco di parametri e dei valori corrispondenti separati da uno spazio (`PROP1=PROP1VAL PROP2=PROP2VAL`).

Nell'elenco dei parametri è necessario includere `EULA=1`. In caso contrario Network Agent non verrà installato.

Se si utilizzano le impostazioni di connessione standard per Kaspersky Security Center e Network Agent nei dispositivi remoti, eseguire il comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` è la chiave per la scrittura dei log. Il log viene creato durante l'installazione di Network Agent e salvato in C:\windows\temp\nag_inst.log.

Oltre a nag_inst.log, l'applicazione crea il file $klssinstlib.log, che contiene il log di installazione. Questo file è archiviato nella cartella %windir%\temp or %temp%. Per la risoluzione dei problemi, l'utente o un esperto del Servizio di assistenza tecnica Kaspersky potrebbe aver bisogno di entrambi i file di log: nag_inst.log e $klssinstlib.log.

Se è necessario specificare la porta per la connessione ad Administration Server, eseguire il comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

Il parametro `SERVERPORT` corrisponde al numero di porta per la connessione ad Administration Server.

I nomi e i possibili valori per i parametri che è possibile utilizzare durante l'installazione di Network Agent in modalità automatica sono elencati nella sezione Parametri di installazione di Network Agent.

Se si desidera aggiornare Network Agent tramite il programma di installazione di Windows, eseguire il seguente comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Installazione di applicazioni in modalità automatica

Per installare un'applicazione in modalità automatica:

1. Nel menu principale accedere a **Individuazione e distribuzione → Distribuzione e assegnazione → Pacchetti di installazione**.
2. Selezionare la casella di controllo accanto al programma di installazione dell'applicazione richiesta o crearne una nuova per l'applicazione.

   Il pacchetto di installazione verrà memorizzato in Administration Server, nella sottocartella Packages della cartella condivisa. A ogni pacchetto di installazione corrisponde una sottocartella distinta.

3. Aprire la cartella che contiene il pacchetto di installazione richiesto in uno dei seguenti modi:

   - Copiando la cartella che corrisponde al pacchetto di installazione appropriato dall'Administration Server nel dispositivo client e aprendo la cartella copiata nel dispositivo client.
   - Aprendo dal dispositivo client la cartella condivisa che corrisponde al pacchetto di installazione desiderato in Administration Server.

Se la cartella condivisa si trova in un dispositivo con sistema operativo Microsoft Windows Vista, selezionare il valore **Disabilitato** per l'impostazione **Controllo dell'account utente: esegui tutti gli amministratori in modalità Approvazione amministratore** (**Start** → **Pannello di controllo** → **Amministrazione** → **Criteri di protezione locali** → **Impostazioni di protezione**).

4. A seconda dell'applicazione selezionata, eseguire le seguenti operazioni:

   - Per Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers e Kaspersky Security Center, aprire la sottocartella exec, quindi eseguire il file eseguibile (con estensione .exe) con la chiave /s.

   - Per le altre applicazioni Kaspersky, eseguire il file eseguibile (con estensione .exe) con l'opzione /s dalla cartella aperta.

L'esecuzione del file eseguibile con le chiavi `EULA=1` e `PRIVACYPOLICY=1` comporta la lettura, la comprensione e l'accettazione dei termini del Contratto di licenza con l'utente finale e dell'Informativa sulla privacy. L'utente è inoltre consapevole che i dati verranno gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy. Il testo del Contratto di licenza e dell'Informativa sulla privacy è incluso nel kit di distribuzione di Kaspersky Security Center Linux. È necessario accettare le condizioni del Contratto di licenza e dell'Informativa sulla privacy per installare l'applicazione o per eseguire l'upgrade da una versione precedente dell'applicazione.

Installazione delle applicazioni tramite pacchetti indipendenti

Kaspersky Security Center consente di creare pacchetti di installazione indipendenti per le applicazioni. Un pacchetto di installazione indipendente è un file eseguibile che può essere posizionato su un server Web, inviato per e-mail o trasferito in altro modo a un dispositivo client. Il file ricevuto può essere eseguito in locale nel dispositivo client per installare un'applicazione senza utilizzare Kaspersky Security Center.

Il Network Agent autonomo per Linux ha una dipendenza facoltativa dall'utilità nmap. Se l'utilità nmap è mancante o è precedente alla versione 6.0, la funzionalità Broadcast DHCP Discover non è supportata.

Per installare un'applicazione utilizzando un pacchetto di installazione indipendente:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.

2. Selezionare la casella di controllo accanto al pacchetto di installazione dell'applicazione richiesta, quindi fare clic sul pulsante **Distribuisci**.

3. Nella finestra visualizzata, selezionare **Utilizzo di un pacchetto indipendente**, quindi fare clic sul pulsante **Avanti**.

   Verrà avviata la Creazione guidata pacchetto di installazione indipendente. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Selezionare l'opzione **Crea pacchetto di installazione indipendente**.

5. Specificare se i dispositivi devono essere spostati in un gruppo di amministrazione dopo l'installazione di Network Agent.

6. Nel passaggio finale della procedura guidata, selezionare un metodo per il trasferimento del pacchetto di installazione indipendente nel dispositivo client, quindi fare clic sull'icona **Fine** per terminare la procedura guidata.

7. Trasferire il pacchetto di installazione indipendente nel dispositivo client.

8. Eseguire il pacchetto di installazione indipendente nel dispositivo client.

L'applicazione verrà installata nel dispositivo client con le impostazioni specificate nel pacchetto indipendente.

Quando si crea un pacchetto di installazione indipendente, questo viene automaticamente pubblicato nel server Web. Il collegamento per il download del pacchetto indipendente viene visualizzato nell'elenco dei pacchetti di installazione indipendenti creati. Se necessario, è possibile annullare la pubblicazione del pacchetto indipendente selezionato e ripubblicarlo sul server Web. Per impostazione predefinita, per il download dei pacchetti di installazione indipendenti viene utilizzata la porta 8060.

Impostazioni del pacchetto di installazione di Network Agent

Per configurare un pacchetto di installazione di Network Agent:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.

   - Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Fare clic sul nome del pacchetto di installazione di Network Agent.

Verrà visualizzata la finestra delle proprietà del pacchetto di installazione di Network Agent.

Le impostazioni di un pacchetto di installazione di di Network Agent sono raggruppate nelle seguenti schede:

- Scheda **Generale**

  Questa scheda mostra le seguenti informazioni sul pacchetto di installazione:

  - Nome pacchetto di installazione

  - Nome e versione dell'applicazione per cui è stato creato il pacchetto di installazione

  - Dimensione del pacchetto di installazione

  - Data di creazione del pacchetto di installazione

  - Percorso della cartella del pacchetto di installazione

- Scheda **Impostazioni**

  Questa scheda presenta le impostazioni necessarie per assicurare il corretto funzionamento di Network Agent subito dopo essere stato installato.

  - Sezione **Impostazioni**

- Installa nella cartella predefinita

  Se questa opzione è selezionata, Network Agent verrà installato nella cartella <Unità>:\Programmi\Kaspersky Lab\NetworkAgent. Se la cartella non esiste, verrà creata automaticamente.

  Per impostazione predefinita, questa opzione è selezionata.

- Installa nella cartella specificata

  Se questa opzione è selezionata, Network Agent verrà installato nella cartella specificata nel campo di immissione.

- Usa password di disinstallazione

  Se questa opzione è abilitata, è possibile immettere la password di disinstallazione (disponibile solo per Network Agent nei dispositivi che eseguono sistemi operativi Windows).

  Per impostazione predefinita, questa opzione è disabilitata.

- Proteggi il servizio Network Agent dalle operazioni non autorizzate di rimozione o terminazione e impedisci la modifica delle impostazioni

  Quando questa opzione è abilitata, dopo l'installazione di Network Agent in un dispositivo gestito, il componente non può essere rimosso o riconfigurato senza i privilegi richiesti. Il servizio Network Agent non può essere arrestato. Questa opzione non ha effetto sui controller di dominio.

  Abilitare questa opzione per proteggere Network Agent sulle workstation gestite con diritti di amministratore locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito

  Se questa opzione è abilitata, tutti gli aggiornamenti e le patch scaricati per Administration Server, Network Agent, Kaspersky Security Center Web Console, server per dispositivi mobili Exchange e server per dispositivi mobili MDM iOS verranno installati automaticamente.

  Se questa opzione è disabilitata, tutti gli aggiornamenti e le patch scaricati verranno installati solo dopo l'impostazione dello stato su *Approvato*. Gli aggiornamenti e le patch con lo stato *Indefinito* non verranno installati.

  Per impostazione predefinita, questa opzione è abilitata.

- Sezione **Connection**

  In questa sezione è possibile configurare la connessione di Network Agent ad Administration Server. Per stabilire una connessione, è possibile utilizzare il protocollo SSL o UDP. Per configurare la connessione, specificare le seguenti impostazioni:

  - Indirizzo di Administration Server

    Indirizzo del dispositivo in cui è installato Administration Server.

  - Numero di porta

Il numero di porta utilizzato per la connessione.

- **Porta SSL**

  Numero di porta utilizzato per la connessione tramite il protocollo SSL.

- **Usa certificato server**

  Se questa opzione è abilitata, l'autenticazione dell'accesso di Network Agent ad Administration Server utilizzerà il file di certificato che è possibile specificare facendo clic sul pulsante **Seleziona file di certificato**.

  Se questa opzione è disabilitata, il file di certificato verrà ricevuto da Administration Server alla prima connessione di Network Agent all'indirizzo specificato nel campo **Indirizzo di Administration Server**.

  È consigliabile non disabilitare questa opzione, poiché la ricezione automatica di un certificato di Administration Server da parte di Network Agent al momento della connessione ad Administration Server è considerata non sicura.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa connessione SSL**

  Se questa opzione è abilitata, la connessione ad Administration Server viene stabilita attraverso una porta sicura tramite SSL.

  Per impostazione predefinita, questa opzione è disabilitata. È consigliabile non disabilitare questa opzione in modo che la connessione rimanga protetta.

- **Usa porta UDP**

  Se questa opzione è abilitata, Network Agent è connesso ad Administration Server tramite una porta UDP. Ciò consente di gestire i dispositivi client e ricevere informazioni in merito.

  La porta UDP deve essere aperta nei dispositivi gestiti in cui è installato Network Agent. È pertanto consigliabile non disabilitare questa opzione.

  Per impostazione predefinita, questa opzione è abilitata.

- **Porta UDP**

  In questo campo è possibile specificare la porta utilizzata per la connessione di Administration Server a Network Agent tramite il protocollo UDP.

  La porta UDP predefinita è 15000.

- **Non usare server proxy**

  Se questa opzione è abilitata, viene utilizzata la connessione diretta per connettere il dispositivo al server di amministrazione.

- **Usa server proxy**

Se questa opzione è abilitata, specificare i parametri del server proxy:

- **Indirizzo server proxy**
- **Porta server proxy**

Se il server proxy richiede l'autenticazione, abilitare l'opzione **Autenticazione server proxy** e specificare il **Nome utente** e la **Password** dell'account con cui viene stabilita la connessione al server proxy. È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

- Per motivi di compatibilità, non è consigliabile specificare le impostazioni di connessione proxy nelle impostazioni del pacchetto di installazione di Network Agent.

- Apri porte di Network Agent in Microsoft Windows Firewall

  Se questa opzione è abilitata, le porte utilizzate da Network Agent vengono aggiunte all'elenco di esclusioni di Microsoft Windows Firewall.

  Per impostazione predefinita, questa opzione è abilitata.

  Questa opzione è disponibile solo per i pacchetti di installazione di Network Agent destinati ai dispositivi che eseguono Windows.

- Sezione **Advanced**

  In questa sezione, è possibile configurare il metodo di utilizzo del gateway di connessione.

  Nel gruppo di impostazioni **Utilizzare Network Agent come gateway di connessione nella rete perimetrale**, è possibile configurare il metodo di connessione tra un dispositivo e Administration Server:

  - Utilizzare Network Agent come gateway di connessione nella rete perimetrale

    Se questa opzione è abilitata, Network Agent viene utilizzato come gateway di connessione nella rete perimetrale per connettersi ad Administration Server, comunicare con esso e assicurare la protezione dei dati in Network Agent durante la trasmissione dei dati.

  - Esegui la connessione ad Administration Server utilizzando un gateway di connessione

    Se questa opzione è abilitata, la connessione ad Administration Server viene stabilita utilizzando un gateway di connessione per ridurre il numero di connessioni ad Administration Server. In questo caso, inserire l'indirizzo del dispositivo che fungerà da gateway di connessione nel campo **Indirizzo gateway connessione**.

  Nel gruppo di impostazioni **Usa VDI (Virtual Desktop Infrastructure)**, è possibile configurare la connessione per Virtual Desktop Infrastructure (VDI) se la rete include macchine virtuali:

  - Abilita modalità dinamica per VDI

    Se questa opzione è abilitata, la modalità dinamica per Virtual Desktop Infrastructure (VDI) sarà abilitata per Network Agent installato in una macchina virtuale.

    Per impostazione predefinita, questa opzione è disabilitata.

  - Ottimizza le impostazioni per VDI

Se questa opzione è abilitata, le seguenti funzionalità sono disabilitate nelle impostazioni di Network Agent:

- Recupero delle informazioni sul software installato
- Recupero delle informazioni sull'hardware
- Recupero delle informazioni sulle vulnerabilità rilevate
- Recupero delle informazioni sugli aggiornamenti richiesti

Per impostazione predefinita, questa opzione è disabilitata.

- Sezione **Tag**

  La sezione **Tag** visualizza un elenco di parole chiave (tag) che possono essere aggiunte ai dispositivi client dopo l'installazione di Network Agent. È possibile aggiungere e rimuovere tag dall'elenco, nonché rinominarli.

  Se la casella di controllo accanto a un tag è selezionata, il tag viene aggiunto automaticamente ai dispositivi gestiti durante l'installazione di Network Agent.

  Se la casella di controllo accanto a un tag è deselezionata, il tag non viene aggiunto automaticamente ai dispositivi gestiti durante l'installazione di Network Agent. È possibile aggiungere manualmente il tag ai dispositivi.

  Rimuovendo un tag dall'elenco, il tag viene rimosso automaticamente da tutti i dispositivi a cui è stato aggiunto.

  Le regole di assegnazione automatica dei tag non sono applicabili ai pacchetti di installazione di Network Agent destinati ai dispositivi in cui viene eseguito Linux e macOS.

- Scheda **Pacchetti indipendenti**

  In questa scheda, è possibile eseguire le seguenti operazioni:

  - Visualizzare l'elenco dei pacchetti di installazione indipendenti disponibili.
  - Pubblicare un pacchetto di installazione indipendente sul server Web facendo clic sul pulsante **Pubblica**. Il pacchetto di installazione indipendente pubblicato è disponibile per il download per gli utenti a cui è stato inviato il collegamento al pacchetto di installazione indipendente.
  - Annullare la pubblicazione di un pacchetto di installazione indipendente sul server Web facendo clic sul pulsante **Annulla pubblicazione**. Il pacchetto di installazione indipendente non pubblicato è disponibile per il download solo per gli amministratori.
  - Scaricare un pacchetto di installazione indipendente nel dispositivo facendo clic sul pulsante **Scarica**.
  - Inviare un messaggio e-mail con il collegamento a un pacchetto di installazione indipendente facendo clic sul pulsante **Invia tramite e-mail**.
  - Rimuovere un pacchetto di installazione indipendente facendo clic sul pulsante **Rimuovi**.

- Scheda **Cronologia revisioni**

  In questa scheda, è possibile visualizzare la cronologia delle revisioni del pacchetto di installazione. È possibile confrontare le revisioni, visualizzare le revisioni, salvare le revisioni in un file e aggiungere e modificare le descrizioni delle revisioni.

Configurazione manuale dell'attività di gruppo per la scansione di un dispositivo con Kaspersky Endpoint Security

L'Avvio rapido guidato crea un'attività di gruppo per la scansione di un dispositivo. Se la pianificazione specificata automaticamente dell'attività di scansione di gruppo non è appropriata per l'organizzazione, è necessario impostare manualmente la pianificazione più adatta per questa attività in base alle regole del luogo di lavoro adottate nell'organizzazione.

Ad esempio, all'attività viene assegnata una pianificazione **Esegui il venerdì alle 19:00** con un'impostazione casuale automatica e la casella di controllo **Esegui attività non effettuate** è deselezionata. Di conseguenza, se i dispositivi nell'organizzazione vengono spenti ad esempio il venerdì alle 18:30, l'attività di scansione del dispositivo non verrà eseguita. In questo caso, è necessario impostare manualmente l'attività di scansione di gruppo.

Gestione dei dispositivi client

Kaspersky Security Center Linux consente di gestire i dispositivi client:

- Visualizzare impostazioni e stati dei dispositivi gestiti, inclusi cluster e array dei server.
- Configurare i punti di distribuzione.
- Gestire le attività.

È possibile utilizzare i gruppi di amministrazione per combinare i dispositivi client in un set che può essere gestito come singola unità. Un dispositivo client può essere incluso in un solo gruppo di amministrazione. I dispositivi possono essere allocati in un gruppo basato automaticamente sulle **Condizioni delle regole**:

- Creazione delle regole di spostamento dei dispositivi.
- Copia delle regole di spostamento dei dispositivi.
- Condizioni di una regola di spostamento dei dispositivi.

È possibile utilizzare selezioni dispositivi per filtrare i dispositivi in base a una condizione. È inoltre possibile eseguire il tagging dei dispositivi per creare selezioni, per trovare dispositivi e per distribuire dispositivi tra i gruppi di amministrazione.

Impostazioni di un dispositivo gestito

Per visualizzare le impostazioni di un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Nell'elenco dei dispositivi gestiti fare clic sul collegamento con il nome del dispositivo richiesto.

Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.

Nella parte superiore della finestra delle proprietà vengono visualizzate le seguenti schede che rappresentano i principali gruppi di impostazioni:

- **Generale**

Questa scheda comprende le seguenti sezioni:

- La sezione **Generale** visualizza informazioni generali sul dispositivo client. Le informazioni sono fornite in base ai dati ricevuti durante l'ultima sincronizzazione del dispositivo client con Administration Server:

  - **Nome**

    In questo campo è possibile visualizzare e modificare il nome di un dispositivo client nel gruppo di amministrazione.

  - **Descrizione**

    In questo campo è possibile immettere un'ulteriore descrizione di un dispositivo client.

  - **Stato dispositivo**

    Stato del dispositivo client assegnato in base ai criteri definiti dall'amministratore per lo stato della protezione anti-virus nel dispositivo e l'attività del dispositivo nella rete.

  - **Proprietario dispositivo**

    Nome del proprietario del dispositivo. È possibile assegnare o rimuovere un utente come proprietario del dispositivo facendo clic sul collegamento **Gestisci proprietario dispositivo**.

  - **Nome completo del gruppo**

    Gruppo di amministrazione che include il dispositivo client.

  - **Ultimo aggiornamento dei database anti-virus**

    Data dell'ultimo aggiornamento delle applicazioni o dei database anti-virus.

  - **Connesso ad Administration Server**

    Data e ora dell'ultima connessione del Network Agent installato nel dispositivo client ad Administration Server.

  - **Ultima visibilità**

    Data e ora in cui il dispositivo è risultato visibile nella rete per l'ultima volta.

  - **Versione di Network Agent**

    Versione del Network Agent installato.

  - **Data creazione**

Data di creazione del dispositivo in Kaspersky Security Center Linux.

- Non eseguire la disconnessione da Administration Server

  Se questa opzione è abilitata, viene mantenuta una connessione continua tra il dispositivo gestito e Administration Server. È consigliabile utilizzare questa opzione se non si utilizzano server push, che offrono questo tipo di connettività.

  Se questa opzione è disabilitata e i server push non sono in uso, il dispositivo gestito si connette ad Administration Server solo per sincronizzare i dati o trasmettere le informazioni.

  Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

  Questa opzione è disabilitata per impostazione predefinita nei dispositivi gestiti. Questa opzione è abilitata per impostazione predefinita nel dispositivo in cui è installato Administration Server e rimane abilitata anche se si tenta di disabilitarla.

- La sezione **Rete** visualizza le seguenti informazioni sulle proprietà di rete del dispositivo client:
  - Indirizzo IP

    Indirizzo IP del dispositivo.

  - Dominio Windows

    Gruppo di lavoro che contiene il dispositivo.

  - Nome DNS

    Nome del dominio DNS del dispositivo client.

  - Nome NetBIOS

    Nome del dispositivo client.

  - **Indirizzo IPv6**
- La sezione **Sistema** fornisce le informazioni sul sistema operativo installato nel dispositivo client.
  - **Sistema operativo**
  - **Architettura della CPU**
  - **Nome dispositivo**
  - Tipo di macchina virtuale

    Produttore della macchina virtuale.

  - Macchina virtuale dinamica come parte di VDI

Questa riga mostra se il dispositivo client è una macchina virtuale dinamica come parte della VDI.

- Nella sezione **Protezione** vengono visualizzate le seguenti informazioni sullo stato corrente della protezione anti-virus nel dispositivo client:
  - **Visibile**

    Stato di visibilità del dispositivo client.

  - **Stato dispositivo**

    Stato del dispositivo client assegnato in base ai criteri definiti dall'amministratore per lo stato della protezione anti-virus nel dispositivo e l'attività del dispositivo nella rete.

  - **Descrizione stato**

    Stato della protezione del dispositivo client e della connessione ad Administration Server.

  - **Stato protezione**

    Questo campo indica lo stato corrente della protezione in tempo reale nel dispositivo client.

    Quando cambia lo stato del dispositivo, il nuovo stato viene visualizzato nella finestra delle proprietà del dispositivo solo dopo la sincronizzazione del dispositivo client con l'Administration Server.

  - **Ultima scansione completa**

    Data e ora dell'ultima scansione malware eseguita nel dispositivo client.

  - **Rilevato virus**

    Numero totale di minacce rilevate nel dispositivo client dall'installazione dell'applicazione di protezione (prima scansione) o dall'ultimo azzeramento del contatore delle minacce.

  - **Oggetti per cui la disinfezione non è riuscita**

    Numero di file non elaborati nel dispositivo client.

    Questo campo ignora il numero di file non elaborati nei dispositivi mobili.

  - **Stato criptaggio disco**

    Stato corrente del criptaggio dei file nelle unità locali del dispositivo. Per una descrizione degli stati consultare la Guida di Kaspersky Endpoint Security for Windows.

    I file possono essere criptati solo nei dispositivi gestiti in cui è installato Kaspersky Endpoint Security for Windows.

- La sezione **Stato dispositivo definito dall'applicazione** fornisce informazioni sullo stato del dispositivo definito dall'applicazione gestita installata nel dispositivo. Lo stato del dispositivo può essere diverso da quello definito da Kaspersky Security Center Linux.

- Applicazioni

  Questa scheda elenca tutte le applicazioni Kaspersky installate nel dispositivo client. Questa scheda contiene i pulsanti **Avvia** e **Arresta** che consentono di avviare e arrestare l'applicazione Kaspersky selezionata (escluso Network Agent). È possibile usare questi pulsanti se la porta 15000 UDP è disponibile nei dispositivi gestiti per la ricezione delle notifiche push da Administration Server. Se il dispositivo gestito non è disponibile per le notifiche push, ma la modalità di connessione continua ad Administration Server è abilitata (l'opzione **Non eseguire la disconnessione da Administration Server** nella sezione **Generale** è abilitata), anche i pulsanti **Avvia** e **Arresta** sono disponibili. Altrimenti, quando si tenta di avviare o arrestare l'applicazione viene visualizzato un messaggio di errore. È inoltre possibile fare clic sul nome dell'applicazione per visualizzare informazioni generali sull'applicazione, un elenco di eventi che si sono verificati nel dispositivo e le impostazioni dell'applicazione.

- Criteri attivi e profili criterio

  In questa scheda, sono elencati i criteri e i profili criterio attualmente assegnato al dispositivo gestito.

- Attività

  Nella scheda **Attività**, è possibile gestire le attività dei dispositivi client: visualizzare l'elenco delle attività esistenti, creare nuove attività, rimuovere, avviare e arrestare le attività, modificare le relative impostazioni e visualizzare i risultati dell'esecuzione. L'elenco delle attività è basato sui dati ricevuti durante l'ultima sessione di sincronizzazione del client con Administration Server. Administration Server richiede i dettagli dello stato delle attività al dispositivo client. Se la porta 15000 UDP è disponibile nel dispositivo gestito per la ricezione delle notifiche push da Administration Server, lo stato dell'attività viene visualizzato e i pulsanti per la gestione delle attività sono abilitati. Se il dispositivo gestito non è disponibile per le notifiche push, ma la modalità di connessione continua ad Administration Server è abilitata (l'opzione **Non eseguire la disconnessione da Administration Server** nella sezione **Generale** è abilitata), anche le azioni con le attività sono disponibili.

  Se la connessione non viene stabilita, lo stato non viene visualizzato e i bottoni vengono disabilitati.

- Eventi

  Nella scheda **Eventi** sono visualizzati gli eventi registrati in Administration Server per il dispositivo client selezionato.

- Problemi di sicurezza

Nella scheda **Problemi di sicurezza**, è possibile visualizzare, modificare e creare problemi di sicurezza per il dispositivo client. I problemi di sicurezza possono essere creati automaticamente, tramite le applicazioni gestite Kaspersky installate nel dispositivo client, o manualmente, dall'amministratore. Se ad esempio alcuni utenti trasferiscono regolarmente malware dalle proprie unità rimovibili nei dispositivi, l'amministratore può creare un problema di sicurezza. L'amministratore può fornire una breve descrizione del caso e le azioni consigliate (ad esempio, azioni disciplinari da intraprendere nei confronti di un utente) nel testo del problema di sicurezza e può aggiungere un collegamento per l'utente o gli utenti.

Un problema di sicurezza per cui sono state eseguite tutte le azioni richieste viene definito *elaborato*. La presenza di problemi di sicurezza non elaborati può essere selezionata come condizione per il passaggio dello stato del dispositivo a *Critico* o *Avviso*.

Questa sezione contiene un elenco dei problemi di sicurezza creati per il dispositivo. I problemi di sicurezza sono classificati in base al tipo e al livello di criticità. Il tipo di un problema di sicurezza è definito dall'applicazione Kaspersky che crea il problema di sicurezza. È possibile evidenziare i problemi di sicurezza elaborati nell'elenco selezionando la casella di controllo nella colonna **Trattati**.

- **Tag**

  Nella sezione **Tag** è possibile gestire l'elenco di parole chiave utilizzate per cercare i dispositivi client: visualizzare l'elenco dei tag esistenti, assegnare tag dall'elenco, configurare le regole per il tagging automatico, aggiungere nuovi tag e rinominare tag esistenti, nonché rimuovere tag.

- **Avanzate**

Questa scheda comprende le seguenti sezioni:

- **Registro delle applicazioni**. In questa sezione, è possibile visualizzare il registro delle applicazioni installate nel dispositivo client e i relativi aggiornamenti, nonché configurare la visualizzazione del registro delle applicazioni.

  Le informazioni sulle applicazioni installate vengono fornite se Network Agent installato nel dispositivo client invia le informazioni richieste ad Administration Server. È possibile configurare l'invio di informazioni ad Administration Server nella finestra delle proprietà di Network Agent o del relativo criterio, nella sezione **Archivi**.

  Facendo clic sul nome di un'applicazione, viene visualizzata una finestra che contiene i dettagli dell'applicazione e un elenco dei pacchetti di aggiornamento installati per l'applicazione.

- **File eseguibili**. In questa sezione sono visualizzati i file eseguibili rilevati nel dispositivo client.

- **Punti di distribuzione**. In questa sezione viene fornito un elenco dei punti di distribuzione con cui interagisce il dispositivo.

  - Esporta in un file

    Fare clic sul pulsante **Esporta in un file** per salvare in un file un elenco di punti di distribuzione con cui interagisce il dispositivo. Per impostazione predefinita, l'applicazione esporta l'elenco di dispositivi in un file CSV.

  - Proprietà

    Fare clic sul pulsante **Proprietà** per visualizzare e configurare il punto di distribuzione con cui interagisce il dispositivo.

- **Registro hardware**. In questa sezione è possibile visualizzare le informazioni relative all'hardware installato nel dispositivo client.

  Se Network Agent è installato in un dispositivo che esegue Windows, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo:

  - RAM
  - Dispositivi di archiviazione di massa
  - Scheda madre
  - CPU
  - Schede di rete
  - Monitor
  - Scheda video
  - Scheda audio

  Se Network Agent è installato in un dispositivo che esegue Linux, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo, se tali informazioni sono fornite dal sistema operativo:

  - Volume totale RAM

- Volume totale dei dispositivi di archiviazione di massa
- Scheda madre
- CPU
- Schede di rete

Se si utilizza un DBMS PostgreSQL, MariaDB o MySQL, la scheda **Eventi** potrebbe mostrare un elenco incompleto di eventi per il dispositivo client selezionato. Questo si verifica quando il DBMS archivia una quantità molto elevata di eventi. È possibile aumentare il numero di eventi visualizzati effettuando una delle seguenti operazioni:

- Rimozione degli eventi non necessari.
- Riduzione del periodo di archiviazione per gli eventi non necessari.

Per visualizzare un elenco completo degli eventi registrati in Administration Server per il dispositivo, utilizzare Rapporti.

Regole di spostamento dei dispositivi

È consigliabile automatizzare l'allocazione dei dispositivi ai gruppi di amministrazione attraverso le *regole di spostamento dei dispositivi*. Una regola di spostamento dei dispositivi comprende tre elementi principali: nome, condizione di esecuzione (espressione logica con gli attributi del dispositivo) e gruppo di amministrazione di destinazione. Una regola sposta un dispositivo nel gruppo di amministrazione di destinazione se gli attributi del dispositivo soddisfano la condizione di esecuzione della regola.

Tutte le regole di spostamento dei dispositivi hanno priorità. L'Administration Server verifica gli attributi del dispositivo per determinare se soddisfano la condizione di esecuzione di ogni regola, in ordine di priorità crescente. Se gli attributi del dispositivo soddisfano la condizione di esecuzione di una regola, il dispositivo viene spostato nel gruppo di destinazione, quindi l'elaborazione della regola è completa per questo dispositivo. Se gli attributi del dispositivo soddisfano le condizioni di più regole, il dispositivo viene spostato nel gruppo di destinazione della regola con la priorità più alta (al livello più alto nell'elenco delle regole).

Le regole di spostamento dei dispositivi possono essere create implicitamente. Ad esempio, nelle proprietà di un pacchetto di installazione o di un'attività di installazione remota è possibile specificare il gruppo di amministrazione in cui deve essere spostato il dispositivo dopo l'installazione di Network Agent. Inoltre, le regole di spostamento dei dispositivi possono essere create esplicitamente dall'amministratore di Kaspersky Security Center Linux nella sezione **Risorse (dispositivi)** → **Regole di spostamento**.

Per impostazione predefinita, una regola di spostamento dei dispositivi viene utilizzata per l'allocazione iniziale dei dispositivi ai gruppi di amministrazione. La regola sposta i dispositivi dal gruppo dei dispositivi non assegnati una sola volta. Se in precedenza un dispositivo era stato spostato da questa regola, la regola non lo sposterà di nuovo, anche se si reinserisce manualmente il dispositivo nel gruppo dei dispositivi non assegnati. Questo è il modo consigliato per applicare le regole di spostamento.

È possibile spostare i dispositivi che sono già stati assegnati ad alcuni gruppi di amministrazione. A tale scopo, nelle proprietà di una regola deselezionare la casella di controllo **Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione**.

L'applicazione delle regole di spostamento a dispositivi che sono già stati assegnati ad alcuni gruppi di amministrazione aumenta considerevolmente il carico sull'Administration Server.

La casella di controllo **Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione** è bloccata nelle proprietà delle regole di spostamento create automaticamente. Tali regole vengono create quando si aggiunge l'attività *Installa applicazione in remoto* o si crea un pacchetto di installazione indipendente.

È possibile creare una regola di spostamento da applicare ripetutamente a un singolo dispositivo.

È consigliabile evitare di spostare ripetutamente un singolo dispositivo da un gruppo all'altro (ad esempio, per applicare uno speciale criterio al dispositivo, eseguire una speciale attività di gruppo o aggiornare il dispositivo attraverso un punto di distribuzione specifico).

Tali scenari non sono supportati, perché comportano un notevole aumento del carico su Administration Server e del traffico di rete. Questi scenari sono anche in conflitto con i principi operativi di Kaspersky Security Center Linux (in particolare nell'area di diritti di accesso, eventi e rapporti). Un'altra soluzione deve ad esempio essere trovata attraverso l'utilizzo di profili criterio, attività per selezioni dispositivi, l'assegnazione di Network Agent in base allo scenario standard.

Creazione delle regole di spostamento dei dispositivi

È possibile impostare regole di spostamento dei dispositivi, ovvero regole che allocano automaticamente i dispositivi ai gruppi di amministrazione.

Per creare una regola di spostamento:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Regole di spostamento**.
2. Fare clic su **Aggiungi**.
3. Nella finestra visualizzata specificare le seguenti impostazioni nella scheda **Generale**:

- **Nome regola**

  Immettere un nome per la nuova regola.

  Se si sta copiando una regola, alla nuova regola è assegnato lo stesso nome della regola di origine, ma al nome viene aggiunto un indice in formato (), ad esempio: (1).

- **Gruppo di amministrazione**

  Selezionare il gruppo di amministrazione in cui devono essere spostati automaticamente i dispositivi.

- **Regola attiva**

  Se questa opzione è abilitata, la regola è abilitata e inizia a funzionare dopo il salvataggio.

  Se questa opzione è disabilitata, la regola viene creata, ma non abilitata. Non funzionerà finché non si abilita questa opzione.

- **Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione**

Se questa opzione è abilitata, solo i dispositivi non assegnati verranno spostati nel gruppo selezionato.

Se questa opzione è disabilitata, i dispositivi che appartengono già ad altri gruppi di amministrazione, nonché i dispositivi non assegnati, verranno spostati nel gruppo selezionato.

- Applica regola

  È possibile selezionare una delle seguenti opzioni:

  - **Esegui una volta per ciascun dispositivo**

    La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri.

  - **Esegui una volta per ciascun dispositivo, quindi a ogni reinstallazione di Network Agent**

    La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri, quindi solo quando Network Agent viene reinstallato in questi dispositivi.

  - **Applica regola in modo continuativo**

    La regola viene applicata in base alla pianificazione impostata automaticamente da Administration Server (in genere, con una frequenza di alcune ore).

4. Nella scheda **Condizioni delle regole**, specificare almeno un criterio in base al quale i dispositivi vengono spostati in un gruppo di amministrazione.

5. Fare clic su **Salva**.

Verrà creata la regola di spostamento. La regola è visualizzata nell'elenco delle regole di spostamento.

Maggiore è la posizione nell'elenco, maggiore sarà la priorità della regola. Per aumentare o diminuire la priorità di una regola di spostamento, spostare la regola rispettivamente in alto o in basso nell'elenco utilizzando il mouse.

Se l'opzione **Applica regola in modo continuativo** è selezionata, la regola di spostamento viene applicata indipendentemente dalle impostazioni di priorità. Tali regole vengono applicate in base alla pianificazione impostata automaticamente da Administration Server.

Se gli attributi del dispositivo soddisfano le condizioni di più regole, il dispositivo viene spostato nel gruppo di destinazione della regola con la priorità più alta (al livello più alto nell'elenco delle regole).

Copia delle regole di spostamento dei dispositivi

È possibile copiare le regole di spostamento, ad esempio se si desidera disporre di più regole identiche per diversi gruppi di amministrazione di destinazione.

Per copiare una regola di spostamento esistente:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Risorse (dispositivi)** → **Regole di spostamento**.

- Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Regole di spostamento**.

Verrà visualizzato l'elenco delle regole di spostamento.

2. Selezionare la casella di controllo accanto alla regola da copiare.

3. Fare clic su **Copia**.

4. Nella finestra visualizzata modificare le seguenti informazioni nella scheda **Generale** (o non apportare modifiche se si desidera solo copiare la regola senza modificarne le impostazioni):

   - Nome regola

     Immettere un nome per la nuova regola.

     Se si sta copiando una regola, alla nuova regola è assegnato lo stesso nome della regola di origine, ma al nome viene aggiunto un indice in formato (), ad esempio: (1).

   - Gruppo di amministrazione

     Selezionare il gruppo di amministrazione in cui devono essere spostati automaticamente i dispositivi.

   - Regola attiva

     Se questa opzione è abilitata, la regola è abilitata e inizia a funzionare dopo il salvataggio.

     Se questa opzione è disabilitata, la regola viene creata, ma non abilitata. Non funzionerà finché non si abilita questa opzione.

   - Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione

     Se questa opzione è abilitata, solo i dispositivi non assegnati verranno spostati nel gruppo selezionato.

     Se questa opzione è disabilitata, i dispositivi che appartengono già ad altri gruppi di amministrazione, nonché i dispositivi non assegnati, verranno spostati nel gruppo selezionato.

   - Applica regola

     È possibile selezionare una delle seguenti opzioni:

     - **Esegui una volta per ciascun dispositivo**

       La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri.

     - **Esegui una volta per ciascun dispositivo, quindi a ogni reinstallazione di Network Agent**

       La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri, quindi solo quando Network Agent viene reinstallato in questi dispositivi.

     - **Applica regola in modo continuativo**

       La regola viene applicata in base alla pianificazione impostata automaticamente da Administration Server (in genere, con una frequenza di alcune ore).

5. Nella scheda **Condizioni delle regole**, specificare almeno un criterio per i dispositivi che si desidera spostare automaticamente.

6. Fare clic su **Salva**.

Verrà creata la nuova regola di spostamento. La regola è visualizzata nell'elenco delle regole di spostamento.

Condizioni di una regola di spostamento dei dispositivi

Quando si crea o copia una regola per spostare i dispositivi client nei gruppi di amministrazione, nella scheda **Condizioni delle regole** si impostano le condizioni per lo spostamento dei dispositivi. Per determinare quali dispositivi spostare, è possibile utilizzare i seguenti criteri:

- Tag assegnati ai dispositivi client.
- Parametri di rete. Ad esempio, è possibile spostare dispositivi con indirizzi IP da un intervallo specificato.
- Applicazioni gestite installate nei dispositivi client, ad esempio Network Agent o Administration Server.
- Macchine virtuali, che sono i dispositivi client.

Di seguito è possibile trovare la descrizione su come specificare queste informazioni in una regola di spostamento dei dispositivi.

Se si specificano più condizioni nella regola, l'operatore logico AND funziona e tutte le condizioni si applicano contemporaneamente. Se non si seleziona alcuna opzione o alcuni campi vengono lasciati vuoti, tali condizioni non si applicano.

Scheda Tag

Nella scheda, è possibile configurare una regola di spostamento dei dispositivi in base ai tag dei dispositivi aggiunti in precedenza alle descrizioni dei dispositivi client. A tale scopo, selezionare i tag richiesti. Inoltre, è possibile abilitare le seguenti opzioni:

- **Applica ai dispositivi senza i tag specificati**

  Se questa opzione è abilitata, tutti i dispositivi con i tag specificati vengono esclusi da una regola di spostamento dei dispositivi. Se questa opzione è disabilitata, la regola di spostamento dei dispositivi si applica ai dispositivi con tutti i tag selezionati.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Applica se almeno uno dei tag specificati corrisponde**

  Se questa opzione è abilitata, una regola di spostamento dei dispositivi si applica ai dispositivi client con almeno uno dei tag selezionati. Se questa opzione è disabilitata, la regola di spostamento dei dispositivi si applica ai dispositivi con tutti i tag selezionati.

  Per impostazione predefinita, questa opzione è disabilitata.

Scheda Rete

In questa scheda, è possibile specificare i dati di rete dei dispositivi considerati da una regola di spostamento dei dispositivi:

- **Nome DNS del dispositivo**

  Nome dominio DNS del dispositivo client che si desidera spostare. Compilare questo campo se la rete include un server DNS.

  Se per il database utilizzato per Kaspersky Security Center Linux sono impostate regole di confronto con distinzione tra maiuscole e minuscole, mantenere le maiuscole e le minuscole quando si specifica un nome DNS del dispositivo. In caso contrario, la regola di spostamento del dispositivo non funzionerà.

- **Dominio DNS**

  Una regola di spostamento dei dispositivi si applica a tutti i dispositivi inclusi nel suffisso DNS principale specificato. Compilare questo campo se la rete include un server DNS.

- **Intervallo IP**

  Se questa opzione è abilitata, è possibile immettere gli indirizzi IP iniziale e finale dell'intervallo IP in cui i dispositivi rilevanti devono essere inclusi.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Indirizzo IP per la connessione ad Administration Server**

  Se questa opzione è abilitata, è possibile impostare gli indirizzi IP tramite i quali i dispositivi client sono collegati all'Administration Server. A tale scopo, specificare l'intervallo IP che include tutti gli indirizzi IP necessari.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Profilo connessione modificato**

  Selezionare uno dei seguenti valori:

  - **Sì**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi client con un profilo di connessione modificato.
  - **No**. La regola di spostamento dei dispositivi si applica solo ai dispositivi client il cui profilo di connessione non è cambiato.
  - **Nessun valore selezionato**. La condizione non si applica.

- **Gestito da un altro Administration Server**

Selezionare uno dei seguenti valori:

- **Sì**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi client gestiti da altri Administration Server. Questi server sono diversi dal server su cui si configura la regola di spostamento dei dispositivi.
- **No**. La regola di spostamento dei dispositivi si applica solo ai dispositivi client gestiti dall'Administration Server corrente.
- **Nessun valore selezionato**. La condizione non si applica.

Scheda Applicazioni

In questa scheda, è possibile configurare una regola di spostamento dei dispositivi in base alle applicazioni gestite e ai sistemi operativi installati nei dispositivi client:

- **Network Agent installato**

  Selezionare uno dei seguenti valori:

  - **Sì**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi client con Network Agent installato.
  - **No**. La regola di spostamento dei dispositivi si applica solo ai dispositivi client in cui Network Agent non è installato.
  - **Nessun valore selezionato**. La condizione non si applica.

- **Applicazioni**

  Specificare quali applicazioni gestite devono essere installate nei dispositivi client, in modo da applicare una regola di spostamento dei dispositivi a tali dispositivi. Ad esempio, è possibile selezionare **Kaspersky Security Center 15 Network Agent** o **Kaspersky Security Center 15 Administration Server**.

  Se non si seleziona alcuna applicazione gestita, la condizione non si applica.

- **Versione del sistema operativo**

  È possibile eliminare i dispositivi client in base alla versione del sistema operativo. A tale scopo, specificare i sistemi operativi che devono essere installati nei dispositivi client. Di conseguenza, una regola di spostamento dei dispositivi si applica ai dispositivi client con i sistemi operativi selezionati.

  Se questa opzione non viene abilitata, la condizione non si applica. Per impostazione predefinita, l'opzione è disabilitata.

- **Dimensioni in bit del sistema operativo**

È possibile selezionare i dispositivi client in base alle dimensioni in bit del sistema operativo. Nel campo **Dimensioni in bit del sistema operativo**, è possibile selezionare uno dei seguenti valori:

- **Sconosciuto**
- **x86**
- **AMD64**
- **IA64**

Per controllare le dimensioni in bit del sistema operativo dei dispositivi client:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul pulsante **Impostazioni colonne** ( ) a destra.
3. Selezionare l'opzione **Dimensioni in bit del sistema operativo**, quindi fare clic sul pulsante **Salva**.

   Successivamente, vengono visualizzate le dimensioni in bit del sistema operativo di ogni dispositivo gestito.

- Versione Service Pack del sistema operativo

  In questo campo è possibile specificare la versione del pacchetto del sistema operativo (nel formato *X.Y*), da cui dipenderà l'applicazione della regola di spostamento al dispositivo. Per impostazione predefinita, non è specificato alcun valore per la versione.

- Certificato utente

  Selezionare uno dei seguenti valori:

  - **Installato**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi mobili con un certificato mobile.
  - **Non installato**. La regola di spostamento dei dispositivi si applica solo ai dispositivi mobili senza un certificato mobile.
  - **Nessun valore selezionato**. La condizione non si applica.

- Build del sistema operativo

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  È possibile specificare se il sistema operativo selezionato deve avere un numero di build uguale, precedente o successivo. È inoltre possibile configurare una regola di spostamento dei dispositivi per tutti i numeri di build ad eccezione di quello specificato.

- Numero di rilascio del sistema operativo

Questa impostazione è applicabile solo ai sistemi operativi Windows.

È possibile specificare se il sistema operativo selezionato deve avere un numero di rilascio uguale, precedente o successivo. È inoltre possibile configurare una regola di spostamento dei dispositivi per tutti i numeri di rilascio ad eccezione di quello specificato.

Scheda Macchine virtuali

In questa scheda, è possibile configurare una regola di spostamento dei dispositivi a seconda che i dispositivi client siano macchine virtuali o facciano parte di una VDI (Virtual Desktop Infrastructure):

- **Questa è una macchina virtuale**

  Nell'elenco a discesa, è possibile selezionare una delle seguenti opzioni:
  - **N/D**. La condizione non si applica.
  - **No**. I dispositivi che non sono macchine virtuali vengono spostati.
  - **Sì**. I dispositivi che sono macchine virtuali vengono spostati.

- **Tipo di macchina virtuale**

- **Parte di Virtual Desktop Infrastructure**

  Nell'elenco a discesa, è possibile selezionare una delle seguenti opzioni:
  - **N/D**. La condizione non si applica.
  - **No**. I dispositivi che non fanno parte della VDI vengono spostati.
  - **Sì**. I dispositivi che fanno parte della VDI vengono spostati.

Scheda Controller di dominio

In questa scheda, è possibile specificare che è necessario spostare i dispositivi inclusi nell'unità organizzativa del dominio. È inoltre possibile spostare i dispositivi da tutte le unità organizzative secondarie dell'unità organizzativa del dominio specificato:

- **Il dispositivo è incluso nella seguente unità organizzativa**

  Se questa opzione è abilitata, viene applicata una regola di spostamento dei dispositivi ai dispositivi dell'unità organizzativa del controller di dominio specificato nell'elenco sotto l'opzione.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Includi unità organizzative secondarie**

Se questa opzione è abilitata, la selezione includerà i dispositivi in tutte le unità organizzative secondarie dell'unità organizzativa del controller di dominio specificato.

Per impostazione predefinita, questa opzione è disabilitata.

- **Sposta i dispositivi dalle unità figlio ai sottogruppi corrispondenti**
- **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati**
- **Elimina sottogruppi non presenti nel dominio**
- **Il dispositivo è incluso nel seguente gruppo di sicurezza del dominio**

  Se questa opzione è abilitata, viene applicata una regola di spostamento dei dispositivi ai dispositivi del gruppo di protezione dei domini specificata nell'elenco sotto l'opzione.

  Per impostazione predefinita, questa opzione è disabilitata.

Aggiunta manuale dei dispositivi a un gruppo di amministrazione

È possibile spostare automaticamente i dispositivi nei gruppi di amministrazione creando regole di spostamento dei dispositivi o manualmente spostando i dispositivi da un gruppo di amministrazione a un altro oppure aggiungendo dispositivi a un gruppo di amministrazione selezionato. Questa sezione descrive come aggiungere manualmente i dispositivi a un gruppo di amministrazione.

Per aggiungere manualmente uno o più dispositivi a un gruppo di amministrazione selezionato:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul collegamento **Percorso corrente:** `<percorso corrente>` sopra l'elenco.
3. Nella finestra visualizzata selezionare il gruppo di amministrazione al quale si desidera aggiungere i dispositivi.
4. Fare clic sul pulsante **Aggiungi dispositivi**.

   Verrà avviato lo Spostamento guidato dispositivi.
5. Creare un elenco dei dispositivi che si desidera aggiungere al gruppo di amministrazione.

   È possibile aggiungere solo i dispositivi per cui sono già state aggiunte informazioni al database di Administration Server durante la connessione del dispositivo o dopo la device discovery.

   Selezionare il modo in cui aggiungere dispositivi all'elenco:

   - Fare clic sul pulsante **Aggiungi dispositivi** e specificare i dispositivi in uno dei seguenti modi:
     - Selezionare i dispositivi dall'elenco dei dispositivi rilevati da Administration Server.
     - Specificare l'indirizzo IP o l'intervallo IP di un dispositivo.
     - Specificare il nome DNS di un dispositivo.

Il campo relativo al nome del dispositivo non deve contenere né spazi né i seguenti caratteri proibiti: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

- Fare clic sul pulsante **Importa dispositivi da file** per importare un elenco di dispositivi da un file .txt. È necessario specificare il nome o l'indirizzo di ciascun dispositivo in una riga separata.

  Il file non deve contenere né spazi né i seguenti caratteri proibiti: , \ / * ' " ; : & ` ~ ! @ # $ ^ ( ) = + [ ] { } | < > %

6. Visualizzare l'elenco dei dispositivi da aggiungere al gruppo di amministrazione. È possibile modificare l'elenco aggiungendo o rimuovendo i dispositivi.

7. Dopo essersi accertati che l'elenco è corretto, fare clic sul pulsante **Avanti**.

La procedura guidata elabora l'elenco dei dispositivi e visualizza il risultato. I dispositivi elaborati correttamente vengono aggiunti al gruppo di amministrazione e visualizzati nell'elenco dei dispositivi con i nomi generati da Administration Server.

Spostamento manuale dei dispositivi o dei cluster in un gruppo di amministrazione

È possibile spostare i dispositivi da un gruppo di amministrazione a un altro o dal gruppo dei dispositivi non assegnati a un gruppo di amministrazione.

È anche possibile spostare cluster o array di server da un gruppo di amministrazione all'altro. Quando si sposta un cluster o un array di server in un altro gruppo, tutti i suoi nodi vengono spostati con esso, perché un cluster e uno qualsiasi dei suoi nodi appartengono sempre allo stesso gruppo di amministrazione. Quando si seleziona un singolo nodo del cluster nella scheda **Risorse (dispositivi)**, il pulsante **Sposta nel gruppo** diventa non disponibile.

Per spostare uno o più dispositivi o cluster in un gruppo di amministrazione selezionato:

1. Aprire il gruppo di amministrazione da cui si desidera spostare i dispositivi. A tale scopo, eseguire una delle operazioni seguenti:

   - Per aprire un gruppo di amministrazione, nel menu principale, accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**, fare clic sul collegamento al percorso nel campo **Percorso corrente** e selezionare un gruppo di amministrazione nel riquadro a sinistra che si apre.

   - Per aprire il gruppo **Dispositivi non assegnati**, nel menu principale passare a **Individuazione e distribuzione** → **Dispositivi non assegnati**.

2. Se il gruppo di amministrazione contiene cluster o array di server, la sezione **Dispositivi gestiti** è divisa in due schede: la scheda **Risorse (dispositivi)** e la scheda **Cluster e array di server**. Aprire la scheda dell'oggetto che si desidera spostare.

3. Selezionare le caselle di controllo accanto ai dispositivi o ai cluster che si desidera spostare in un altro gruppo.

4. Fare clic sul pulsante **Sposta nel gruppo**.

5. Nella gerarchia dei gruppi di amministrazione, selezionare la casella di controllo accanto al gruppo di amministrazione in cui si desidera spostare i dispositivi o i cluster selezionati.

6. Fare clic sul pulsante **Sposta**.

I dispositivi o i cluster selezionati verranno spostati nel gruppo di amministrazione selezionato.

Informazioni sui cluster e sugli array di server

Kaspersky Security Center Linux supporta la tecnologia cluster. Se Network Agent invia ad Administration Server informazioni che confermano che l'applicazione installata in un dispositivo client fa parte di un array di server, il dispositivo client diventa un nodo del cluster.

Se un gruppo di amministrazione contiene cluster o array di server, la pagina **Dispositivi gestiti** mostra due schede: una per i singoli dispositivi e una per i cluster e gli array di server. Dopo che i dispositivi gestiti vengono rilevati come nodi del cluster, il cluster viene aggiunto come oggetto singolo alla scheda **Cluster e array di server**.

I nodi del cluster o dell'array di server sono elencati nella scheda **Dispositivi**, insieme ad altri dispositivi gestiti. È possibile visualizzare le proprietà dei nodi come dispositivi singoli ed eseguire altre operazioni, ma non è possibile eliminare un nodo del cluster o spostarlo in un altro gruppo di amministrazione separatamente dal relativo cluster. È solo possibile eliminare o spostare un intero cluster.

È possibile eseguire le seguenti operazioni con cluster o array di server:

- Visualizzare le proprietà
- Spostare il cluster o l'array di server in un altro gruppo di amministrazione

  Quando si sposta un cluster o un array di server in un altro gruppo, tutti i suoi nodi vengono spostati con esso, perché un cluster e uno qualsiasi dei suoi nodi appartengono sempre allo stesso gruppo di amministrazione.

- Elimina

  È ragionevole eliminare un cluster o un array di server solo quando il cluster o l'array di server non esiste più nella rete dell'organizzazione. Se un cluster è ancora visibile nella rete e Network Agent e l'applicazione di protezione Kaspersky è ancora installata nei nodi del cluster, Kaspersky Security Center Linux restituisce automaticamente il cluster eliminato e i relativi nodi all'elenco dei dispositivi gestiti.

Proprietà di un cluster o di un array di server

Per visualizzare le impostazioni di un cluster o di un array di server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti** → **Cluster e array di server**.

   Viene visualizzato l'elenco dei cluster e degli array di server.

2. Fare clic sul nome del cluster o dell'array di server richiesto.

Verrà visualizzata la finestra delle proprietà del cluster o dell'array di server selezionato.

Generale

La sezione **Generale** mostra informazioni generali sul cluster o sull'array di server. Le informazioni sono fornite in base ai dati ricevuti durante l'ultima sincronizzazione dei nodi del cluster con Administration Server:

- **Nome**
- **Descrizione**
- Dominio Windows

  Dominio o gruppo di lavoro di Windows, che contiene il cluster o l'array di server.

- Nome NetBIOS

  Nome di rete Windows del cluster o dell'array di server.

- Nome DNS

  Nome del dominio DNS del cluster o dell'array di server.

Attività

Nella scheda **Attività**, è possibile gestire le attività assegnate al cluster o all'array di server: visualizzare l'elenco delle attività esistenti, creare nuove attività, rimuovere, avviare e arrestare le attività, modificare le impostazioni delle attività e visualizzare i risultati dell'esecuzione. Le attività elencate si riferiscono all'applicazione di protezione Kaspersky installata nei nodi del cluster. Kaspersky Security Center Linux riceve l'elenco delle attività e i dettagli sullo stato delle attività dai nodi del cluster. Se non viene stabilita una connessione, lo stato non viene visualizzato.

Nodi

Questa scheda mostra un elenco di nodi inclusi nel cluster o nell'array di server. È possibile fare clic sul nome di un nodo per visualizzare la finestra delle proprietà del dispositivo.

Applicazione Kaspersky

La finestra delle proprietà può contenere anche schede aggiuntive con le informazioni e le impostazioni relative all'applicazione di protezione Kaspersky installata nei nodi del cluster.

Regolazione di punti di distribuzione e gateway di connessione

Una struttura di gruppi di amministrazione in Kaspersky Security Center Linux esegue le seguenti funzioni:

- Imposta l'ambito dei criteri

  È disponibile un metodo alternativo per l'applicazione delle impostazioni appropriate nei dispositivi, utilizzando i *profili criterio*.

- Imposta l'ambito delle attività di gruppo

Esiste un approccio alla definizione dell'ambito delle attività di gruppo che non è basato su una gerarchia di gruppi di amministrazione: l'utilizzo di attività per selezioni dispositivi e di attività per dispositivi specifici.

- Imposta i diritti di accesso a dispositivi, Administration Server virtuali e Administration Server secondari
- Assegna i punti di distribuzione

Al momento della creazione della struttura dei gruppi di amministrazione, è necessario tenere conto della topologia della rete dell'organizzazione per l'assegnazione ottimale dei punti di distribuzione. La distribuzione ottimale dei punti di distribuzione consente di ridurre il traffico nella rete dell'organizzazione.

A seconda dello schema dell'organizzazione e della topologia di rete, le seguenti configurazioni standard possono essere applicate alla struttura dei gruppi di amministrazione:

- Singola sede
- Più sedi remote di piccole dimensioni

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Configurazione standard dei punti di distribuzione: singola sede

In una configurazione standard con una singola sede, tutti i dispositivi si trovano nella rete dell'organizzazione e sono visibili reciprocamente. La rete dell'organizzazione può comprendere diversi componenti (reti o segmenti di rete) connessi tramite canali con larghezza di banda ridotta.

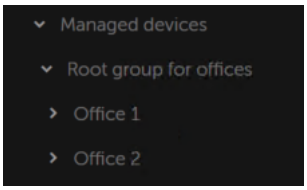
Sono disponibili i seguenti metodi per creare la struttura dei gruppi di amministrazione:

- Creazione della struttura dei gruppi di amministrazione tenendo conto della topologia di rete. La struttura dei gruppi di amministrazione potrebbe non riflettere la topologia di rete alla perfezione. Una corrispondenza tra i diversi componenti della rete e alcuni gruppi di amministrazione può essere sufficiente. È possibile utilizzare l'assegnazione automatica dei punti di distribuzione o assegnarli manualmente.
- Creazione della struttura dei gruppi di amministrazione senza tenere conto della topologia di rete. In questo caso è necessario disabilitare l'assegnazione automatica dei punti di distribuzione e quindi assegnare a uno o più dispositivi il ruolo di punti di distribuzione per un gruppo di amministrazione radice in ciascun componente della rete, ad esempio per il gruppo **Dispositivi gestiti**. Tutti i punti di distribuzione saranno allo stesso livello e avranno lo stesso ambito che comprende tutti i dispositivi della rete dell'organizzazione. In questo caso, tutti i Network Agent si connetteranno al punto di distribuzione con il percorso più vicino. Il percorso di un punto di distribuzione è monitorabile con l'utilità tracert.

Configurazione standard dei punti di distribuzione: più sedi remote di piccole dimensioni

Questa configurazione standard prevede la presenza di diverse sedi remote, che possono comunicare con la sede centrale via Internet. Ogni sede remota è situata dietro il NAT, ovvero la connessione da una sede remota all'altra non è possibile perché le sedi sono isolate tra loro.

La configurazione deve essere riflessa nella struttura dei gruppi di amministrazione: è necessario creare un gruppo di amministrazione distinto per ogni sede remota (i gruppi **Sede 1** e **Sede 2** nella figura seguente).



Le sedi remote sono incluse nella struttura dei gruppi di amministrazione

È necessario assegnare uno o più punti di distribuzione a ogni gruppo di amministrazione che corrisponde a una sede. I punti di distribuzione devono essere dispositivi nella sede remota con una quantità sufficiente di spazio libero su disco. I dispositivi distribuiti nel gruppo **Sede 1**, ad esempio, accederanno ai punti di distribuzione assegnati al gruppo di amministrazione **Sede 1**.

Se alcuni utenti si spostano fisicamente tra le sedi con i loro computer portatili, è necessario selezionare due o più dispositivi (oltre ai punti di distribuzione esistenti) in ogni sede remota e assegnare loro il ruolo di punti di distribuzione per un gruppo di amministrazione di primo livello (**Gruppo radice per le sedi** nella figura precedente).

Esempio: un computer portatile è distribuito nel gruppo di amministrazione **Sede 1** e quindi viene spostato fisicamente nella sede che corrisponde al gruppo di amministrazione **Sede 2**. Dopo lo spostamento del portatile, Network Agent tenta di accedere ai punti di distribuzione assegnati al gruppo **Sede 1**, ma tali punti di distribuzione non sono disponibili. Network Agent inizia quindi a tentare di accedere ai punti di distribuzione che sono stati assegnati al **Gruppo radice per le sedi**. Poiché le sedi remote sono isolate tra loro, i tentativi di accedere ai punti di distribuzione assegnati al gruppo di amministrazione **Gruppo radice per le sedi** avranno esito positivo solo quando Network Agent tenta di accedere ai punti di distribuzione nel gruppo **Sede 2**. In altre parole, il computer portatile rimarrà nel gruppo di amministrazione che corrisponde alla sede iniziale, ma utilizzerà il punto di distribuzione della sede in cui si trova fisicamente al momento.

Calcolo del numero e configurazione dei punti di distribuzione

Più dispositivi client contiene una rete, maggiore è il numero dei punti di distribuzione richiesti. È consigliabile non disabilitare l'assegnazione automatica dei punti di distribuzione. Quando è abilitata l'assegnazione automatica dei punti di distribuzione, Administration Server assegna i punti di distribuzione se il numero dei dispositivi client è ampio e definisce la configurazione.

Utilizzo di punti di distribuzione assegnati in modo esclusivo

Se si prevede di utilizzare alcuni dispositivi specifici come punti di distribuzione (ovvero, server assegnati in modo esclusivo), è possibile scegliere di non utilizzare l'assegnazione automatica dei punti di distribuzione. In questo caso, verificare che i dispositivi a cui assegnare il ruolo di punti di distribuzione dispongano di un volume sufficiente di spazio libero su disco, che non vengano arrestati regolarmente e che la modalità di sospensione sia disabilitata.

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–100	1
Più di 100	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Utilizzo di dispositivi client standard (workstation) come punti di distribuzione

Se si prevede di utilizzare dispositivi client standard (ovvero, workstation) come punti di distribuzione, è consigliabile assegnare i punti di distribuzione come indicato nelle tabelle seguenti per evitare un carico eccessivo sui canali di comunicazione e su Administration Server:

Numero di workstation che operano come punti di distribuzione in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Numero di workstation che operano come punti di distribuzione in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–30	1
31–300	2
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Se un punto di distribuzione viene arrestato (o non è disponibile per altri motivi), i dispositivi gestiti nel relativo ambito possono accedere ad Administration Server per gli aggiornamenti.

Assegnazione automatica di punti di distribuzione

È consigliabile assegnare automaticamente i punti di distribuzione. In questo caso, Kaspersky Security Center Linux selezionerà autonomamente a quali dispositivi assegnare i punti di distribuzione.

Per assegnare automaticamente i punti di distribuzione:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Selezionare l'opzione **Assegna i punti di distribuzione automaticamente**.

   Se è abilitata l'assegnazione automatica dei dispositivi come punti di distribuzione, non è possibile configurare i punti di distribuzione manualmente, né modificare l'elenco dei punti di distribuzione.

4. Fare clic sul pulsante **Salva**.

Administration Server assegna e configura i punti di distribuzione automaticamente.

Assegnazione manuale di punti di distribuzione

Kaspersky Security Center Linux consente di assegnare manualmente ai dispositivi il ruolo di punti di distribuzione.

È consigliabile assegnare automaticamente i punti di distribuzione. In questo caso, Kaspersky Security Center Linux selezionerà autonomamente a quali dispositivi assegnare i punti di distribuzione. Tuttavia, se per qualche motivo non è possibile assegnare automaticamente i punti di distribuzione (se ad esempio si desidera utilizzare i server assegnati in modo esclusivo), è possibile assegnare i punti di distribuzione manualmente dopo averne calcolato il numero ed eseguito la configurazione.

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Per assegnare manualmente a un dispositivo il ruolo di punto di distribuzione:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Selezionare l'opzione **Assegna i punti di distribuzione manualmente**.

4. Fare clic sul pulsante **Assegna**.

5. Selezionare il dispositivo che si desidera rendere un punto di distribuzione.

   Quando si seleziona un dispositivo, tenere presenti le funzionalità operative dei punti di distribuzione e i requisiti definiti per il dispositivo che opera come punto di distribuzione.

6. Selezionare il gruppo di amministrazione da includere nell'ambito del punto di distribuzione selezionato.

7. Fare clic sul pulsante **OK**.

   Il punto di distribuzione aggiunto sarà visualizzato nell'elenco dei punti di distribuzione, nella sezione **Punti di distribuzione**.

8. Fare clic sul nuovo punto di distribuzione aggiunto nell'elenco per aprire la relativa finestra delle proprietà.

9. Configurare il punto di distribuzione nella finestra delle proprietà:

   - La sezione **Generale** contiene le impostazioni per l'interazione tra il punto di distribuzione e i dispositivi client.

     - **Porta SSL**

       Numero della porta SSL per la connessione criptata tra i dispositivi client e il punto di distribuzione tramite SSL.

       Per impostazione predefinita, viene utilizzata la porta 13000.

     - **Usa multicast**

Se questa opzione è abilitata, verrà utilizzata la modalità IP multicast per la distribuzione automatica dei pacchetti di installazione ai dispositivi client del gruppo.

Il multicast IP riduce il tempo necessario per installare un'applicazione da un pacchetto di installazione in un gruppo di dispositivi client, ma aumenta il tempo di installazione quando si installa un'applicazione in un singolo dispositivo client.

- **Indirizzo IP multicast**

  Indirizzo IP che verrà utilizzato per la modalità multicast. È possibile definire un indirizzo IP nell'intervallo da 224.0.0.0 a 239.255.255.255

  Per impostazione predefinita Kaspersky Security Center Linux assegna automaticamente un indirizzo IP multicast univoco all'interno dell'intervallo specificato.

- **Numero di porta IP multicast**

  Numero di porta per la modalità IP multicast.

  Il numero di porta predefinito è 15001. Se il dispositivo in cui è installato Administration Server è specificato come punto di distribuzione, per impostazione predefinita viene utilizzata la porta 13001 per la connessione SSL.

- **Indirizzo del punto di distribuzione per i dispositivi remoti**

  L'indirizzo IPv4 attraverso il quale i dispositivi remoti si connettono al punto di distribuzione.

- **Distribuisci aggiornamenti**

  Gli aggiornamenti vengono distribuiti ai dispositivi gestiti dalle seguenti sorgenti:

  - Questo punto di distribuzione se l'opzione è abilitata.
  - Altri punti di distribuzione, Administration Server o server degli aggiornamenti Kaspersky se l'opzione è disabilitata.

  Se si utilizzano i punti di distribuzione per distribuire gli aggiornamenti, è possibile risparmiare traffico riducendo il numero di download. È inoltre possibile alleggerire il carico su Administration Server e ridistribuirlo tra i punti di distribuzione. È possibile calcolare il numero di punti di distribuzione per la propria rete in modo da ottimizzare il traffico e il carico.

  Se si disabilita questa opzione, il numero di download degli aggiornamenti e il carico su Administration Server potrebbero aumentare. Per impostazione predefinita, questa opzione è abilitata.

- **Distribuisci pacchetti di installazione**

I pacchetti di installazione vengono distribuiti ai dispositivi gestiti dalle seguenti sorgenti:

- Questo punto di distribuzione se l'opzione è abilitata.
- Altri punti di distribuzione, Administration Server o server degli aggiornamenti Kaspersky se l'opzione è disabilitata.

Se si utilizzano i punti di distribuzione per distribuire i pacchetti di installazione, è possibile risparmiare traffico riducendo il numero di download. È inoltre possibile alleggerire il carico su Administration Server e ridistribuirlo tra i punti di distribuzione. È possibile calcolare il numero di punti di distribuzione per la propria rete in modo da ottimizzare il traffico e il carico.

Se si disabilita questa opzione, il numero di download dei pacchetti di installazione e il carico su Administration Server potrebbero aumentare. Per impostazione predefinita, questa opzione è abilitata.

- **Esegui server push**

  In Kaspersky Security Center Linux un punto di distribuzione può fungere da server push per i dispositivi gestiti tramite il protocollo mobile e per i dispositivi gestiti da Network Agent. È ad esempio necessario abilitare un server push se si desidera forzare la sincronizzazione dei dispositivi KasperskyOS con Administration Server. Un server push ha lo stesso ambito dei dispositivi gestiti del punto di distribuzione in cui è abilitato il server push. Se sono stati assegnati più punti di distribuzione per lo stesso gruppo di amministrazione, è possibile abilitare il server push in ciascuno dei punti di distribuzione. In questo caso, Administration Server bilancia il carico tra i punti di distribuzione.

- **Porta server push**

  Il numero di porta per il server push. È possibile specificare il numero di qualsiasi porta non occupata.

- Nella sezione **Ambito** specificare i gruppi di amministrazione ai quali il punto di distribuzione distribuirà gli aggiornamenti.

- Nella sezione **Sorgente degli aggiornamenti**, è possibile selezionare una sorgente degli aggiornamenti per il punto di distribuzione:

  - **Sorgente degli aggiornamenti**

    Selezionare una sorgente degli aggiornamenti per il punto di distribuzione:

    - Per consentire al punto di distribuzione di ricevere gli aggiornamenti da Administration Server, selezionare **Recupera da Administration Server**:
    - Per consentire al punto di distribuzione di ricevere gli aggiornamenti tramite un'attività, selezionare **Usa l'attività di download degli aggiornamenti**, quindi specificare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*:
      - Se tale attività esiste già nel dispositivo, selezionare l'attività nell'elenco.
      - Se tale attività non esiste ancora nel dispositivo, fare clic sul collegamento **Crea attività** per creare un'attività. Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

- **Scarica file diff**

  Questa opzione consente di abilitare la funzionalità di download dei file diff.

  Per impostazione predefinita, questa opzione è abilitata.

- Se i punti di distribuzione utilizzano un server proxy durante la connessione a Internet, nella sottosezione **Impostazioni connessione Internet** è possibile specificare le seguenti impostazioni:

  - **Usa server proxy**

    Se questa casella di controllo è selezionata, nei campi di immissione è possibile configurare la connessione al server proxy.

    Per impostazione predefinita, questa casella di controllo è deselezionata.

  - **Indirizzo server proxy**

    Indirizzo del server proxy.

  - **Numero di porta**

    Il numero di porta utilizzato per la connessione.

  - **Ignora il server proxy per gli indirizzi locali**

    Se questa opzione è abilitata, non viene utilizzato alcun server proxy per la connessione ai dispositivi nella rete locale.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Autenticazione server proxy**

    Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

    Per impostazione predefinita, questa casella di controllo è deselezionata.

  - **Nome utente**

    Account utente con cui viene stabilita la connessione al server proxy.

  - **Password**

    Password dell'account con cui verrà eseguita l'attività.

- Nella sezione **Proxy KSN** è possibile configurare l'applicazione per l'utilizzo del punto di distribuzione per l'inoltro delle richieste KSN dai dispositivi gestiti:

  - **Abilita proxy KSN da parte del punto di distribuzione**

Il servizio proxy KSN viene eseguito nel dispositivo utilizzato come punto di distribuzione. Utilizzare questa funzionalità per ridistribuire e ottimizzare il traffico nella rete.

Il punto di distribuzione invia le statistiche KSN, elencate nell'informativa di Kaspersky Security Network, a Kaspersky.

Per impostazione predefinita, questa opzione è disabilitata. L'attivazione di questa opzione ha effetto solo se le opzioni **Usa Administration Server come server proxy** e **Accetto di utilizzare Kaspersky Security Network** sono abilitate nella finestra delle proprietà di Administration Server.

È possibile assegnare il nodo di un cluster attivo-passivo a un punto di distribuzione e abilitare il proxy KSN in tale nodo.

- Inoltra richieste KSN ad Administration Server

  Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti ad Administration Server.

  Per impostazione predefinita, questa opzione è abilitata.

- Accedi a KSN Cloud/KPSN direttamente tramite Internet

  Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti a KSN Cloud o KPSN. Anche le richieste KSN generate nello stesso punto di distribuzione vengono inviate direttamente a KSN Cloud o KPSN.

- Ignora impostazioni del server proxy durante la connessione a KPSN

  Abilitare questa opzione se le impostazioni del server proxy sono configurate nelle proprietà del punto di distribuzione o nel criterio di Network Agent ma l'architettura di rete richiede l'utilizzo diretto di KPSN. In caso contrario, le richieste dalle applicazioni gestite non possono raggiungere KPSN.

  Questa opzione è disponibile se si seleziona l'opzione **Accedi a KSN Cloud/KPSN direttamente tramite Internet**.

- Porta

  Numero della porta TCP utilizzata dai dispositivi gestiti per la connessione al server proxy KSN. Il numero di porta predefinito è 13111.

- Usa porta UDP

  Se è necessario che i dispositivi gestiti si connettano al server proxy KSN attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in Porta UDP. Per impostazione predefinita, questa opzione è abilitata.

- Porta UDP

  Numero della porta UDP utilizzata dai dispositivi gestiti per la connessione al server proxy KSN. La porta UDP predefinita per la connessione al server proxy KSN è la 15111.

- Nella sezione **Gateway di connessione**, è possibile configurare il punto di distribuzione in modo che funga da gateway per la connessione tra le istanze di Network Agent e Administration Server:

- **Gateway di connessione**

  Se non è possibile stabilire una connessione diretta tra Administration Server e Network Agent a causa dell'organizzazione della rete, è possibile utilizzare il punto di distribuzione come porta di connessione tra Administration Server e i Network Agent.

  Abilitare questa opzione se è necessario che il punto di distribuzione funga da gateway di connessione tra Network Agent e Administration Server. Per impostazione predefinita, questa opzione è disabilitata.

- **Stabilisci connessione al gateway da Administration Server (se il gateway è in una rete perimetrale)**

  Se Administration Server si trova al di fuori della zona perimetrale (DMZ), sulla rete locale, i Network Agent installati nei dispositivi remoti non possono connettersi ad Administration Server. È possibile usare un punto di distribuzione come gateway di connessione con connettività inversa (Administration Server stabilisce una connessione al punto di distribuzione).

  Abilitare questa opzione se è necessario connettere Administration Server al gateway di connessione in DMZ.

- **Apri porta locale per Kaspersky Security Center Web Console**

  Abilitare questa opzione se è necessario che il gateway di connessione in DMZ apra una porta per la Web Console che si trova in DMZ o su Internet. Specificare il numero di porta che verrà utilizzato per la connessione da Web Console al punto di distribuzione. Il numero di porta predefinito è 13299.

  Questa opzione è disponibile se si abilita l'opzione **Stabilisci connessione al gateway da Administration Server (se il gateway è in una rete perimetrale)**.

Quando i dispositivi mobili vengono connessi ad Administration Server tramite il punto di distribuzione che funge da gateway di connessione, è possibile abilitare le seguenti opzioni:

- **Apri porta per i dispositivi mobili (autenticazione SSL solo di Administration Server)**

  Abilitare questa opzione se è necessario che il gateway di connessione apra una porta per i dispositivi mobili e specificare il numero di porta che i dispositivi mobili utilizzeranno per la connessione al punto di distribuzione. Il numero di porta predefinito è 13292. Il dispositivo mobile controllerà il certificato di Administration Server. Quando si stabilisce la connessione, viene autenticato solo Administration Server.

- **Apri porta per i dispositivi mobili (autenticazione SSL bidirezionale)**

Abilitare questa opzione se è necessario che il gateway di connessione apra una porta che verrà utilizzata per l'autenticazione bidirezionale di Administration Server e dei dispositivi mobili. Il dispositivo mobile controllerà il certificato di Administration Server e Administration Server controllerà il certificato del dispositivo mobile. Specificare i seguenti parametri:

- Numero di porta che i dispositivi mobili useranno per la connessione al punto di distribuzione. Il numero di porta predefinito è 13293.
- Nomi di dominio DNS del gateway di connessione che verranno utilizzati dai dispositivi mobili. Separare i nomi di dominio con virgole. I nomi di dominio specificati verranno inclusi nel certificato del punto di distribuzione. Se i nomi di dominio usati dai dispositivi mobili non corrispondono al nome comune nel certificato del punto di distribuzione, i dispositivi mobili non si connettono al punto di distribuzione.

  Il nome di dominio DNS predefinito è il nome di dominio completo del gateway di connessione.

In entrambi i casi, i certificati vengono verificati quando si stabilisce la sessione TLS solo nel punto di distribuzione. I certificati non vengono inoltrati per la verifica da parte dell'Administration Server. Dopo aver stabilito una sessione TLS con il dispositivo mobile, il punto di distribuzione utilizza il certificato di Administration Server per creare un tunnel per la sincronizzazione tra il dispositivo mobile e Administration Server. Se si apre la porta per l'autenticazione SSL bidirezionale, l'unico modo per distribuire il certificato del dispositivo mobile è tramite un pacchetto di installazione.

- Configurare il polling del controller di dominio in base al punto di distribuzione.
  - Polling del controller di dominio

    È possibile abilitare la device discovery per i controller di dominio.

    Se si seleziona l'opzione **Abilita polling controller di dominio**, è possibile selezionare i controller di dominio per il polling e anche specificare la pianificazione del polling per gli stessi.

    Se si utilizza un punto di distribuzione Linux, nella sezione **Esegui polling di domini specifici**, fare clic su **Aggiungi**, quindi specificare l'indirizzo e le credenziali utente del controller di dominio.

    Se si utilizza un punto di distribuzione Windows, è possibile selezionare una delle seguenti opzioni:

    - **Esegui polling dominio corrente**
    - **Esegui polling di tutta la foresta di dominio**
    - **Esegui polling di domini specifici**

- Configurare il polling degli intervalli IP da parte del punto di distribuzione.
  - Polling intervallo IP

Adesso è possibile abilitare Device discovery per gli intervalli IPv4 e le reti IPv6.

Se si abilita l'opzione **Abilita polling intervallo**, è possibile aggiungere gli intervalli esaminati e impostare la relativa pianificazione. È possibile aggiungere intervalli IP all'elenco degli intervalli esaminati.

Se si abilita l'opzione **Usa Zeroconf per il polling delle reti IPv6**, il punto di distribuzione esegue automaticamente il polling della rete IPv6 utilizzando le reti zero-configuration (definite anche *Zeroconf*). In questo caso, gli intervalli IP specificati vengono ignorati perché il punto di distribuzione esegue il polling dell'intera rete. L'opzione **Usa Zeroconf per il polling delle reti IPv6** è disponibile se nel punto di distribuzione viene eseguito Linux. Per utilizzare il polling ipv6 Zeroconf, è necessario installare l'utilità avahi-browse nel punto di distribuzione.

- Nella sezione **Avanzate** specificare la cartella che il punto di distribuzione deve utilizzare per archiviare i dati distribuiti.
  - **Usa cartella predefinita**

    Se questa opzione è selezionata, l'applicazione utilizza la cartella di installazione di Network Agent nel punto di distribuzione.

  - **Usa cartella specificata**

    Se questa opzione è selezionata, nel campo sottostante è possibile specificare il percorso della cartella. È possibile specificare una cartella locale nel punto di distribuzione oppure una cartella in qualsiasi dispositivo nella rete aziendale.

    L'account utente utilizzato nel punto di distribuzione per eseguire Network Agent deve disporre di accesso in lettura e scrittura alla cartella specificata.

10. Fare clic sul pulsante **OK**.

    I dispositivi selezionati opereranno come punti di distribuzione.

Modifica dell'elenco dei punti di distribuzione per un gruppo di amministrazione

È possibile visualizzare l'elenco dei punti di distribuzione assegnati a un gruppo di amministrazione specifico e modificare l'elenco aggiungendo o rimuovendo punti di distribuzione.

Per visualizzare e modificare l'elenco dei punti di distribuzione assegnati a un gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Nel campo **Percorso corrente** sopra l'elenco dei dispositivi gestiti, fare clic sul collegamento del percorso.
3. Nel riquadro visualizzato a sinistra, selezionare un gruppo di amministrazione per cui si desidera visualizzare i punti di distribuzione assegnati.

   Viene abilitata la voce di menu **Punti di distribuzione**.
4. Nel menu principale accedere a **Risorse (dispositivi)** → **Punti di distribuzione**.

5. Per aggiungere nuovi punti di distribuzione per il gruppo di amministrazione, fare clic sul pulsante **Assegna**.

6. Per rimuovere i punti di distribuzione assegnati, selezionare i dispositivi nell'elenco e fare clic sul pulsante **Annulla assegnazione**.

A seconda delle modifiche, i nuovi punti di distribuzione verranno aggiunti all'elenco o i punti di distribuzione esistenti verranno rimossi dall'elenco.

Abilitazione di un server push

In Kaspersky Security Center Linux un punto di distribuzione può fungere da server push per i dispositivi gestiti tramite il protocollo mobile e per i dispositivi gestiti da Network Agent. È ad esempio necessario abilitare un server push se si desidera forzare la sincronizzazione dei dispositivi KasperskyOS con Administration Server. Un server push ha lo stesso ambito dei dispositivi gestiti del punto di distribuzione in cui è abilitato il server push. Se sono stati assegnati più punti di distribuzione per lo stesso gruppo di amministrazione, è possibile abilitare il server push in ciascuno dei punti di distribuzione. In questo caso, Administration Server bilancia il carico tra i punti di distribuzione.

È consigliabile utilizzare i punti di distribuzione come server push per garantire la continuità della connessione tra un dispositivo gestito e Administration Server. La continuità della connessione è necessaria per alcune operazioni, come l'esecuzione e l'arresto di attività locali, la ricezione di statistiche per un'applicazione gestita o la creazione di un tunnel. Se si utilizza un punto di distribuzione come server push, non è necessario utilizzare l'opzione **Non eseguire la disconnessione da Administration Server** nei dispositivi gestiti o inviare pacchetti alla porta UDP di Network Agent.

Un server push supporta il carico massimo di 50.000 connessioni simultanee.

Per abilitare il server push in un punto di distribuzione:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Fare clic sul nome del punto di distribuzione in cui si desidera abilitare il server push.

   Verrà visualizzata la finestra delle proprietà del punto di distribuzione.

4. Nella sezione **Generale** abilitare l'opzione **Esegui server push**.

5. Nel campo **Porta server push** digitare il numero di porta. È possibile specificare il numero di qualsiasi porta non occupata.

6. Nel campo **Indirizzo per host remoti** specificare l'indirizzo IP o il nome del dispositivo del punto di distribuzione.

7. Fare clic sul pulsante **OK**.

Il server push è abilitato nel punto di distribuzione selezionato.

Informazioni sugli stati dei dispositivi

Kaspersky Security Center Linux assegna uno stato a ciascun dispositivo gestito. Lo stato specifico dipende dal rispetto delle condizioni definite dall'utente. In alcuni casi, durante l'assegnazione di uno stato a un dispositivo, Kaspersky Security Center Linux prende in considerazione il flag di visibilità del dispositivo nella rete (vedere la tabella seguente). Se Kaspersky Security Center Linux non rileva un dispositivo nella rete entro due ore, il flag di visibilità del dispositivo è impostato su *Non visibile*.

Gli stati sono i seguenti:

- *Critico* o *Critico / Visibile*
- *Avviso* o *Avviso / Visibile*
- *OK* o *OK / Visibile*

La tabella seguente elenca le condizioni predefinite da soddisfare per assegnare a un dispositivo lo stato *Critico* o *Avviso*, con tutti i possibili valori.

Condizioni per l'assegnazione di uno stato a un dispositivo

Condizione	Descrizione della condizione	Valori disponibili
Applicazione di protezione non installata	Network Agent è installato nel dispositivo, ma un'applicazione di protezione non è installata.	• L'interruttore è attivato. • L'interruttore è disattivato.
Troppi virus rilevati	Nel dispositivo sono stati rilevati alcuni virus da parte di un'attività per il rilevamento dei virus, ad esempio l'attività Scansione malware, e il numero di virus trovati supera il valore specificato.	Più di 0.
Livello protezione in tempo reale diverso da quello impostato dall'amministratore	Il dispositivo è visibile nella rete, ma il livello della protezione in tempo reale è diverso dal livello impostato (nella condizione) dall'amministratore per lo stato del dispositivo.	• Arrestata. • Sospesa. • In esecuzione.
Scansione malware non eseguita da molto tempo	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma né l'attività *Scansione malware* né un'attività di scansione locale sono state eseguite nell'intervallo di tempo specificato. La condizione è applicabile solo ai dispositivi che sono stati aggiunti al database di Administration Server 7 giorni o più di 7 giorni prima.	Più di 1 giorno.
I database non sono aggiornati	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma i database anti-virus non vengono aggiornati nel dispositivo nell'intervallo di tempo specificato. La condizione è applicabile solo ai dispositivi che sono stati aggiunti al database di Administration Server un giorno o più di un giorno prima.	Più di 1 giorno.
Connessione non eseguita da molto tempo	Network Agent è installato nel dispositivo, ma il dispositivo non viene connesso a un Administration Server nell'intervallo di tempo specificato, perché il dispositivo era spento.	Più di 1 giorno.
Rilevate minacce attive	Il numero di oggetti non elaborati nella cartella **Minacce attive** è superiore al valore specificato.	Più di 0 elementi.
È necessario il riavvio	Il dispositivo è visibile nella rete, ma un'applicazione richiede il riavvio del dispositivo da un periodo superiore all'intervallo di tempo specificato e per uno dei motivi selezionati.	Più di 0 minuti.
Applicazioni incompatibili installate	Il dispositivo è visibile nella rete, ma l'inventario software eseguito tramite Network Agent ha rilevato applicazioni incompatibili installate nel dispositivo.	• L'interruttore è disattivato. • L'interruttore è attivato.
La licenza è scaduta	Il dispositivo è visibile nella rete, ma la licenza è scaduta.	• L'interruttore è disattivato. • L'interruttore è attivato.
La licenza sta per scadere	Il dispositivo è visibile nella rete, ma la licenza nel dispositivo scadrà tra un numero di giorni inferiore rispetto a quello specificato.	Più di 0 giorni.
Stato criptaggio	Network Agent è installato nel dispositivo, ma il risultato del criptaggio dispositivo è uguale al	• Non è conforme al

non valido	valore specificato.	criterio a causa di un rifiuto dell'utente (solo per i dispositivi esterni). • Non è conforme al criterio a causa di un errore. • È richiesto il riavvio per l'applicazione del criterio. • Non è specificato alcun criterio di criptaggio. • Non supportato. • Quando viene applicato il criterio.
Problemi di sicurezza non elaborati rilevati	Sono stati rilevati nel dispositivo alcuni problemi di sicurezza non elaborati. I problemi di sicurezza possono essere creati automaticamente, tramite le applicazioni gestite Kaspersky installate nel dispositivo client, o manualmente, dall'amministratore.	• L'interruttore è disattivato. • L'interruttore è attivato.
Stato dispositivo definito dall'applicazione	Lo stato del dispositivo è definito dall'applicazione gestita.	• L'interruttore è disattivato. • L'interruttore è attivato.
Spazio su disco esaurito nel dispositivo	Lo spazio disponibile sul disco nel dispositivo è inferiore al valore specificato o il dispositivo non può essere sincronizzato con Administration Server. Lo stato *Critico* o *Avviso* diventa *OK* quando il dispositivo viene sincronizzato con Administration Server e lo spazio disponibile nel dispositivo è maggiore o uguale al valore specificato.	Più di 0 MB.
Il dispositivo è diventato non gestito	Durante la device discovery, il dispositivo è stato riconosciuto come visibile nella rete, ma più di tre tentativi di sincronizzazione con Administration Server hanno avuto esito negativo.	• L'interruttore è disattivato. • L'interruttore è attivato.
Protezione disattivata	Il dispositivo è visibile nella rete, ma l'applicazione di protezione nel dispositivo è stata disabilitata per un periodo superiore all'intervallo di tempo specificato. In questo caso, lo stato dell'applicazione di protezione è *interrotto* o *non riuscito* e differisce dai seguenti: *avvio*, *esecuzione* o *sospensione*.	Più di 0 minuti.
Applicazione di protezione non in esecuzione	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma non è in esecuzione.	• L'interruttore è disattivato. • L'interruttore è attivato.

Kaspersky Security Center Linux consente di configurare la selezione automatica dello stato di un dispositivo in un gruppo di amministrazione quando vengono soddisfatte le condizioni specificate. Quando vengono soddisfatte le condizioni specificate, al dispositivo client viene assegnato uno dei seguenti stati: *Critico* o *Avviso*. Quando le condizioni specificate non vengono soddisfatte, al dispositivo client viene assegnato lo stato *OK*.

Diversi stati possono corrispondere ai diversi valori di una condizione. Ad esempio, per impostazione predefinita, se alla condizione **I database non sono aggiornati** è associato il valore **Più di 3 giorni**, al dispositivo client sarà assegnato lo stato *Avviso*; se il valore è **Più di 7 giorni**, verrà assegnato lo stato *Critico*.

Se si esegue l'upgrade di Kaspersky Security Center Linux dalla versione precedente, i valori della condizione **I database non sono aggiornati** per l'assegnazione dello stato *Critico* o *Avviso* restano invariati.

Quando Kaspersky Security Center Linux assegna uno stato a un dispositivo, per alcune condizioni (vedere la colonna Descrizione della condizione) viene preso in considerazione il flag di visibilità. Ad esempio, se a un dispositivo gestito è stato assegnato lo stato *Critico* perché è stata soddisfatta la condizione I database non sono aggiornati e successivamente è stato impostato il flag di visibilità per il dispositivo, al dispositivo viene assegnato lo stato *OK*.

Configurazione del passaggio degli stati del dispositivo

È possibile modificare le condizioni per assegnare lo stato *Critico* o *Avviso* a un dispositivo.

Per abilitare la modifica dello stato del dispositivo in Critico:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nell'elenco dei gruppi visualizzato fare clic sul collegamento con il nome di un gruppo per cui si desidera modificare lo stato del dispositivo.
3. Nella finestra delle proprietà visualizzata selezionare la scheda **Stato dispositivo**.
4. Nel riquadro sinistro selezionare **Critico**.
5. Nel riquadro destro, nella sezione **Imposta su Critico se è specificato**, abilitare la condizione per il passaggio di un dispositivo allo stato *Critico*.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio principale.

6. Selezionare il pulsante di opzione accanto alla condizione nell'elenco.
7. Nell'angolo superiore sinistro dell'elenco fare clic sul pulsante **Modifica**.
8. Impostare il valore richiesto per la condizione selezionata.

   I valori non possono essere impostati per tutte le condizioni.

9. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Critico*.

Per abilitare la modifica dello stato del dispositivo in Avviso:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nell'elenco dei gruppi visualizzato fare clic sul collegamento con il nome di un gruppo per cui si desidera modificare lo stato del dispositivo.
3. Nella finestra delle proprietà visualizzata selezionare la scheda **Stato dispositivo**.
4. Nel riquadro sinistro selezionare **Avviso**.
5. Nel riquadro destro, nella sezione **Imposta su Avviso se è specificato**, abilitare la condizione per il passaggio di un dispositivo allo stato *Avviso*.

È possibile modificare solo le impostazioni che non sono bloccate nel criterio principale.

6. Selezionare il pulsante di opzione accanto alla condizione nell'elenco.
7. Nell'angolo superiore sinistro dell'elenco fare clic sul pulsante **Modifica**.
8. Impostare il valore richiesto per la condizione selezionata.

   I valori non possono essere impostati per tutte le condizioni.
9. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Avviso*.

Selezioni dispositivi

Le *selezioni dispositivi* sono uno strumento per filtrare i dispositivi in base a condizioni specifiche. È possibile utilizzare le selezioni dispositivi per gestire diversi dispositivi, ad esempio per visualizzare un rapporto solo su questi dispositivi o per spostare tutti questi dispositivi in un altro gruppo.

Kaspersky Security Center Linux offre un'ampia gamma di *selezioni predefinite* (ad esempio, **Dispositivi con stato Critico**, **Protezione disattivata**, **Rilevate minacce attive**). Le selezioni predefinite non possono essere eliminate. È inoltre possibile creare e configurare ulteriori *selezioni definite dall'utente*.

Nelle selezioni definite dall'utente è possibile impostare l'ambito di ricerca e selezionare tutti i dispositivi, i dispositivi gestiti o i dispositivi non assegnati. I parametri di ricerca sono specificati nelle condizioni. Nella selezione dispositivi è possibile creare diverse condizioni con parametri di ricerca differenti. È ad esempio possibile creare due condizioni e specificare intervalli IP diversi in ciascuna di esse. Se vengono specificate più condizioni, una selezione visualizza i dispositivi che soddisfano una qualsiasi delle condizioni. Al contrario, i parametri di ricerca in una condizione vengono sovrapposti. Se in una condizione si specificano sia un intervallo IP che il nome di un'applicazione installata, verranno visualizzati solo i dispositivi in cui è installata l'applicazione e con un indirizzo IP che appartiene all'intervallo specificato.

Visualizzazione dell'elenco dei dispositivi da una selezione di dispositivi

Kaspersky Security Center Linux consente di visualizzare l'elenco dei dispositivi da una selezione di dispositivi.

Per visualizzare l'elenco dei dispositivi dalla selezione di dispositivi:

1. Nel menu principale, passare alla sezione **Risorse (dispositivi)** → **Selezioni dispositivi** o **Individuazione e distribuzione** → **Selezioni dispositivi**.
2. Nell'elenco delle selezioni fare clic sul nome della selezione di dispositivi.

   La pagina mostra una tabella con le informazioni sui dispositivi inclusi nella selezione di dispositivi.
3. È possibile raggruppare e filtrare i dati della tabella dei dispositivi come segue:

   - Fare clic sull'icona delle impostazioni (⚙), quindi selezionare le colonne da visualizzare nella tabella.
   - Fare clic sull'icona del filtro (▽), quindi specificare e applicare il criterio di filtro nel menu richiamato.

Viene visualizzata la tabella filtrata dei dispositivi.

È possibile selezionare uno o più dispositivi nella selezione di dispositivi e fare clic sul pulsante **Nuova attività** per creare un'attività che verrà applicata a tali dispositivi.

Per spostare i dispositivi selezionati della selezione di dispositivi in un altro gruppo di amministrazione, fare clic sul pulsante **Sposta nel gruppo**, quindi selezionare il gruppo di amministrazione di destinazione.

Creazione di una selezione dispositivi

Per creare una selezione dispositivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Selezioni dispositivi**.

   Verrà visualizzata una pagina con un elenco di selezioni dispositivi.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Impostazioni della selezione dispositivi**.

3. Immettere il nome della nuova selezione.

4. Specificare il gruppo che contiene i dispositivi da includere nella selezione di dispositivi:

   - **Trova qualsiasi dispositivo**: ricerca dei dispositivi che soddisfano i criteri di selezione e inclusi nel gruppo **Dispositivi gestiti** o **Dispositivi non assegnati**.
   - **Trova dispositivi gestiti**: ricerca dei dispositivi che soddisfano i criteri di selezione e inclusi nel gruppo **Dispositivi gestiti**.
   - **Trova dispositivi non assegnati**: ricerca dei dispositivi che soddisfano i criteri di selezione e inclusi nel gruppo **Dispositivi non assegnati**.

   È possibile abilitare la casella di controllo **Includi i dati degli Administration Server secondari** per abilitare la ricerca dei dispositivi che soddisfano i criteri di selezione e gestiti dagli Administration Server secondari.

5. Fare clic sul pulsante **Aggiungi**.

6. Nella finestra visualizzata specificare le condizioni che devono essere soddisfatte per includere i dispositivi in questa selezione, quindi fare clic sul pulsante **OK**.

7. Fare clic sul pulsante **Salva**.

La selezione dispositivi viene creata e aggiunta all'elenco delle selezioni dispositivi.

Configurazione di una selezione dispositivi

Per configurare una selezione dispositivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Selezioni dispositivi**.

   Verrà visualizzata una pagina con un elenco di selezioni dispositivi.

2. Selezionare la selezione di dispositivi definita dall'utente pertinente e fare clic sul pulsante **Proprietà**.

   Verrà visualizzata la finestra **Impostazioni della selezione dispositivi**.

3. Nella scheda **Generale**, fare clic sul collegamento **Nuova condizione**.

4. Specificare le condizioni da soddisfare per l'inclusione dei dispositivi nella selezione.

5. Fare clic sul pulsante **Salva**.

Le impostazioni verranno applicate e salvate.

Di seguito sono descritte le condizioni per l'assegnazione dei dispositivi a una selezione. Le condizioni vengono combinate tramite l'operatore logico OR: la selezione conterrà i dispositivi conformi ad almeno una delle condizioni elencate.

Generale

Nella sezione **Generale** è possibile modificare il nome della condizione di selezione e specificare se tale condizione deve essere invertita:

Inverti condizione selezione

Se questa opzione è abilitata, la condizione di selezione specificata verrà invertita. La selezione includerà tutti i dispositivi che non soddisfano la condizione.

Per impostazione predefinita, questa opzione è disabilitata.

Infrastruttura di rete

Nella sottosezione **Rete**, è possibile specificare i criteri che verranno utilizzati per includere i dispositivi nella selezione in base ai dati della rete:

- Nome dispositivo

  Nome di rete Windows (nome NetBIOS) del dispositivo o indirizzo IPv4 o IPv6.

- Dominio

  Visualizza tutti i dispositivi inclusi nel gruppo di lavoro specificato.

- Gruppo di amministrazione

  Visualizza i dispositivi inclusi nel gruppo di amministrazione specificato.

- Descrizione

Testo contenuto nella finestra delle proprietà del dispositivo: nel campo **Descrizione** della sezione **Generale**.

Per inserire il testo nel campo **Descrizione**, è possibile utilizzare i seguenti caratteri:

- All'interno di una parola:
  - *****. Sostituisce qualsiasi stringa con qualsiasi numero di caratteri.

    Esempio:

    Per descrivere parole come **Server** o **Server's**, è possibile immettere **Server***.
  - **?.** Sostituisce qualsiasi carattere singolo.

    Esempio:

    per descrivere frasi come **SUSE Linux Enterprise Server 12** o **SUSE Linux Enterprise Server 15** è possibile immettere **SUSE Linux Enterprise Server 1?**.

    Non è possibile utilizzare l'asterisco (*****) o il punto interrogativo (**?**) come primo carattere nella query.
- Per trovare più parole:
  - Spazio. Visualizza tutti i dispositivi le cui descrizioni contengono una delle parole elencate.

    Esempio:

    Per trovare una frase contenente le parole **Secondario** o **Virtuale**, è possibile includere la riga **Secondario Virtuale** nella query.
  - **+**. Quando una parola è preceduta dal segno +, tutti i risultati della ricerca conterranno tale parola.

    Esempio:

    Per trovare una frase contenente sia **Secondario** che **Virtuale**, immettere la query **+Secondario+Virtuale**.
  - **-**. Quando una parola è preceduta dal segno -, nessun risultato della ricerca conterrà tale parola.

    Esempio:

    Per trovare una frase contenente **Secondario** e non contenente **Virtuale**, immettere la query **+Secondario-Virtuale**.
  - **"<testo>"**. Verranno visualizzati i risultati che contengono il testo racchiuso tra virgolette.

    Esempio:

    Per trovare una frase contenente la combinazione di parole **Server secondario**, è possibile immettere **"Server secondario"** nella query.

- Intervallo IP

  Se questa opzione è abilitata, è possibile immettere gli indirizzi IP iniziale e finale dell'intervallo IP in cui i dispositivi rilevanti devono essere inclusi.

  Per impostazione predefinita, questa opzione è disabilitata.

- Gestito da un altro Administration Server

Selezionare uno dei seguenti valori:

- **Sì**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi client gestiti da altri Administration Server. Questi server sono diversi dal server su cui si configura la regola di spostamento dei dispositivi.
- **No**. La regola di spostamento dei dispositivi si applica solo ai dispositivi client gestiti dall'Administration Server corrente.
- **Nessun valore selezionato**. La condizione non si applica.

Nella sottosezione **Controller di dominio**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'appartenenza a un dominio:

- Il dispositivo si trova in un'unità organizzativa del dominio

  Se questa opzione è abilitata, la selezione includerà i dispositivi dell'unità organizzativa del dominio specificata nel campo di immissione.

  Per impostazione predefinita, questa opzione è disabilitata.

- Il dispositivo fa parte del gruppo di sicurezza del dominio

  Se questa opzione è abilitata, la selezione includerà i dispositivi del gruppo di sicurezza del dominio specificato nel campo di immissione.

  Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Attività di rete**, è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base alle relative attività della rete:

- Funge da punto di distribuzione

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. La selezione include i dispositivi che operano come punti di distribuzione.
  - **No**. I dispositivi che operano come punti di distribuzione non sono inclusi nella selezione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Non eseguire la disconnessione da Administration Server

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Abilitata**. La selezione includerà i dispositivi in cui la casella di controllo **Non eseguire la disconnessione da Administration Server** è selezionata.
  - **Disabilitata**. La selezione includerà i dispositivi in cui la casella di controllo **Non eseguire la disconnessione da Administration Server** è deselezionata.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Profilo connessione cambiato

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. La selezione includerà i dispositivi che hanno eseguito la connessione ad Administration Server dopo la modifica del profilo di connessione.
  - **No**. La selezione non includerà i dispositivi che hanno eseguito la connessione ad Administration Server dopo la modifica del profilo di connessione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Ultima connessione ad Administration Server

  È possibile utilizzare questa casella di controllo per impostare un criterio di ricerca per i dispositivi in base all'ora dell'ultima connessione ad Administration Server.

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare l'intervallo di tempo (data e ora) durante il quale è stata stabilita l'ultima connessione tra Network Agent installato nel dispositivo client e Administration Server. La selezione includerà i dispositivi che rientrano nell'intervallo specificato.

  Se questa casella di controllo è deselezionata, il criterio non verrà applicato.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Rilevati nuovi dispositivi durante il polling della rete

  Cerca nuovi dispositivi rilevati dal polling della rete negli ultimi giorni.

  Se questa opzione è abilitata, la selezione includerà soltanto i nuovi dispositivi rilevati dalla device discovery nel numero di giorni specificato nel campo **Periodo di rilevamento (giorni)**.

  Se questa opzione è disabilitata, la selezione includerà tutti i dispositivi rilevati dalla device discovery.

  Per impostazione predefinita, questa opzione è disabilitata.

- Il dispositivo è visibile

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. L'applicazione include nella selezione i dispositivi attualmente visibili nella rete.
  - **No**. L'applicazione include nella selezione i dispositivi attualmente invisibili nella rete.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

Stati dispositivi

Nella sottosezione **Stato del dispositivo gestito**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base alla descrizione dello stato dei dispositivi ottenuta da un'applicazione gestita:

- Stato dispositivo

Elenco a discesa in cui è possibile selezionare uno degli stati del dispositivo: *OK*, *Critico* o *Avviso*.

- **Stato protezione in tempo reale**

  Elenco a discesa in cui è possibile selezionare lo stato della protezione in tempo reale. I dispositivi con lo stato della protezione in tempo reale specificato vengono inclusi nella selezione.

- **Descrizione stato del dispositivo**

  In questo campo è possibile selezionare le caselle di controllo accanto alle condizioni che, se soddisfatte, assegnano al dispositivo uno dei seguenti stati: *OK*, *Critico* o *Avviso*.

Nella sezione **Stato dei componenti nelle applicazioni gestite**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base agli stati dei componenti nelle applicazioni gestite:

- **Stato prevenzione fughe di dati**

  Cercare i dispositivi in base allo stato di prevenzione della perdita dei dati (*Nessun dato dal dispositivo*, *Arrestata*, *Avvio in corso*, *Sospesa*, *In esecuzione*, *Non riuscito*).

- **Stato protezione server di collaborazione**

  Cercare i dispositivi in base allo stato della protezione della collaborazione server (*Nessun dato dal dispositivo*, *Arrestata*, *Avvio in corso*, *Sospesa*, *In esecuzione*, *Non riuscito*).

- **Stato protezione anti-virus server di posta**

  Cercare i dispositivi in base allo stato della protezione dei server di posta (*Nessun dato dal dispositivo*, *Arrestata*, *Avvio in corso*, *Sospesa*, *In esecuzione*, *Non riuscito*).

- **Stato Endpoint Sensor**

  Cercare i dispositivi in base allo stato del componente Sensore Endpoint (*Nessun dato dal dispositivo*, *Arrestata*, *Avvio in corso*, *Sospesa*, *In esecuzione*, *Non riuscito*).

Nella sezione **Problemi che influiscono sullo stato nelle applicazioni gestite** è possibile specificare i criteri per l'inclusione dei dispositivi nella selezione in base all'elenco dei possibili problemi rilevati da un'applicazione gestita. Se è presente almeno un problema selezionato in un dispositivo, il dispositivo verrà incluso nella selezione. Quando si seleziona un problema elencato per diverse applicazioni, è possibile selezionare automaticamente questo problema in tutti gli elenchi.

È possibile selezionare le caselle di controllo relative alle descrizioni degli stati dall'applicazione gestita. Alla ricezione di questi stati, i dispositivi verranno inclusi nella selezione. Quando si seleziona uno stato elencato per diverse applicazioni, è possibile selezionare automaticamente questo stato in tutti gli elenchi.

Dettagli di sistema

Nella sezione **Sistema operativo** è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base al tipo di sistema operativo.

- Tipo di piattaforma

  Se la casella di controllo è selezionata, è possibile selezionare un sistema operativo dall'elenco. I dispositivi in cui sono installati i sistemi operativi specificati saranno inclusi nei risultati della ricerca.

- Versione Service Pack del sistema operativo

  In questo campo è possibile specificare la versione del pacchetto del sistema operativo (nel formato *X.Y*), da cui dipenderà l'applicazione della regola di spostamento al dispositivo. Per impostazione predefinita, non è specificato alcun valore per la versione.

- Dimensioni in bit del sistema operativo

  Nell'elenco a discesa è possibile selezionare l'architettura del sistema operativo da cui dipenderà l'applicazione della regola di spostamento al dispositivo (**Sconosciuto**, **x86**, **AMD64** o **IA64**). Per impostazione predefinita, non è selezionata alcuna opzione nell'elenco, pertanto l'architettura del sistema operativo non è definita.

- Build del sistema operativo

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  Numero di build del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un numero di build uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti i numeri di build ad eccezione di quello specificato.

- Numero di rilascio del sistema operativo

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  Identificatore della versione (ID) del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un ID di rilascio uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti gli ID di rilascio ad eccezione di quello specificato.

Nella sezione **Macchine virtuali** è possibile configurare i criteri per l'inclusione dei dispositivi nella selezione in base al fatto che siano macchine virtuali o che facciano parte di Microsoft Virtual Desktop Infrastructure (VDI):

- Questa è una macchina virtuale

  Dall'elenco a discesa è possibile selezionare le seguenti opzioni:

  - **Indefinito**.
  - **No**. I dispositivi che non sono macchine virtuali vengono trovati.
  - **Sì**. Vengono trovati i dispositivi che sono macchine virtuali.

- Tipo di macchina virtuale

  Nell'elenco a discesa è possibile selezionare il produttore della macchina virtuale.

  Questo elenco a discesa è disponibile se è selezionato il valore **Sì** o **Non importante** nell'elenco a discesa **Questa è una macchina virtuale**.

- Parte di Virtual Desktop Infrastructure

  Dall'elenco a discesa è possibile selezionare le seguenti opzioni:

  - **Indefinito**.
  - **No**. Vengono trovati i dispositivi che non fanno parte di Virtual Desktop Infrastructure.
  - **Sì**. Vengono trovati i dispositivi che fanno parte di Microsoft Virtual Desktop Infrastructure (VDI).

Nella sottosezione **Registro hardware**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'hardware installato:

Assicurarsi che l'utilità lshw sia installata nei dispositivi Linux da cui si desidera recuperare i dettagli dell'hardware. I dettagli dell'hardware recuperati dalle macchine virtuali potrebbero essere incompleti a seconda dell'hypervisor utilizzato.

- Dispositivo

  Nell'elenco a discesa è possibile selezionare un tipo di unità. Tutti i dispositivi con questa unità verranno inclusi nei risultati della ricerca.

  Il campo supporta la ricerca full-text.

- Fornitore

  Nell'elenco a discesa è possibile selezionare il nome di un produttore dell'unità. Tutti i dispositivi con questa unità verranno inclusi nei risultati della ricerca.

  Il campo supporta la ricerca full-text.

- Nome dispositivo

  Il dispositivo con il nome specificato verrà incluso nella selezione.

- Descrizione

  Descrizione del dispositivo o dell'unità hardware. I dispositivi con la descrizione specificata in questo campo verranno inclusi nella selezione.

  La descrizione di un dispositivo in qualsiasi formato può essere immessa nella finestra delle proprietà del dispositivo. Il campo supporta la ricerca full-text.

- Produttore dispositivo

Nome del produttore del dispositivo. I dispositivi del produttore specificato in questo campo verranno inclusi nella selezione.

È possibile inserire il nome del produttore nella finestra delle proprietà di un dispositivo.

- **Numero di serie**

  Tutte le unità hardware con il numero di serie specificato in questo campo verranno incluse nella selezione.

- **Numero di inventario**

  L'apparecchiatura con il numero di inventario specificato in questo campo verrà inclusa nella selezione.

- **Utente**

  Tutte le unità hardware dell'utente specificato in questo campo verranno incluse nella selezione.

- **Posizione**

  Posizione del dispositivo o dell'unità hardware (ad esempio nella sede principale o in una filiale). I computer o gli altri dispositivi distribuiti al percorso specificato in questo campo verranno inclusi nella selezione.

  È possibile descrivere il percorso di un dispositivo in qualsiasi formato nella finestra delle proprietà del dispositivo.

- **Frequenza di clock della CPU (in MHz) da**

  La frequenza di clock minima di una CPU. I dispositivi con una CPU che corrisponde all'intervallo di frequenza di clock specificati nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Frequenza di clock della CPU (in MHz) a**

  La frequenza di clock massima di una CPU. I dispositivi con una CPU che corrisponde all'intervallo di frequenza di clock specificati nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Numero di core CPU virtuali, da**

  Il numero minimo di core CPU virtuali. I dispositivi con una CPU che corrisponde all'intervallo del numero di core virtuali specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Numero di core CPU virtuali, a**

  Il numero massimo di core CPU virtuali. I dispositivi con una CPU che corrisponde all'intervallo del numero di core virtuali specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Volume disco rigido (GB) da**

  Il volume minimo del disco rigido sul dispositivo. I dispositivi con un disco rigido che corrisponde all'intervallo di volumi nei campi di immissione (compresi) verranno inclusi nella selezione.

- Volume disco rigido (GB) a

  Il volume massimo del disco rigido sul dispositivo. I dispositivi con un disco rigido che corrisponde all'intervallo di volumi nei campi di immissione (compresi) verranno inclusi nella selezione.

- Dimensione RAM (MB) da

  La dimensione minima della RAM del dispositivo. I dispositivi con una RAM che corrisponde all'intervallo di dimensione specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

- Dimensione RAM (MB) a

  La dimensione massima della RAM del dispositivo. I dispositivi con una RAM che corrisponde all'intervallo di dimensione specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

Dettagli software di terze parti

Nella sottosezione **Registro delle applicazioni**, è possibile impostare i criteri di ricerca dei dispositivi in base alle applicazioni installate:

- Nome applicazione

  Elenco a discesa da cui è possibile selezionare un'applicazione. I dispositivi in cui è installata l'applicazione specificata sono inclusi nella selezione.

- Versione applicazione

  Campo di immissione in cui è possibile specificare la versione dell'applicazione selezionata.

- Fornitore

  Elenco a discesa da cui è possibile selezionare il produttore di un'applicazione installata nel dispositivo.

- Stato applicazione

  Elenco a discesa da cui è possibile selezionare lo stato di un'applicazione (*Installata*, *Non installata*). Verranno inclusi nella selezione i dispositivi in cui è installata o non è installata l'applicazione specificata, in base allo stato selezionato.

- Trova per aggiornamento

  Se questa opzione è abilitata, la ricerca verrà eseguita utilizzando i dettagli degli aggiornamenti per le applicazioni installate nei dispositivi. Dopo aver selezionato la casella di controllo, i campi **Nome applicazione**, **Versione applicazione** e **Stato applicazione** diventano rispettivamente **Nome aggiornamento**, **Versione aggiornamento** e **Stato**.

  Per impostazione predefinita, questa opzione è disabilitata.

- Nome dell'applicazione di protezione incompatibile

Elenco a discesa da cui è possibile selezionare applicazioni di protezione di terze parti. Durante la ricerca, i dispositivi in cui è installata l'applicazione specificata sono inclusi nella selezione.

- Tag applicazione

  Nell'elenco a discesa è possibile selezionare il tag di un'applicazione. Tutti i dispositivi che hanno applicazioni installate con il tag selezionato nella descrizione sono inclusi nella selezione dispositivi.

- Applica ai dispositivi senza i tag specificati

  Se questa opzione è abilitata, la selezione includerà i dispositivi con descrizioni che non contengono alcuno dei tag selezionati.

  Se questa opzione è disabilitata, il criterio non viene applicato.

  Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Vulnerabilità e aggiornamenti**, è possibile specificare i criteri per l'inclusione dei dispositivi nella selezione in base all'origine di Windows Update:

WUA è passato ad Administration Server

È possibile selezionare una delle seguenti opzioni di ricerca nell'elenco a discesa:

- **Sì**. Se questa opzione è selezionata, i risultati di ricerca includeranno i dispositivi che ricevono gli aggiornamenti tramite Windows Update da Administration Server.
- **No**. Se questa opzione è selezionata, i risultati di ricerca includeranno i dispositivi che ricevono gli aggiornamenti tramite Windows Update da altre origini.

Dettagli delle applicazioni Kaspersky

Nella sottosezione **Applicazioni Kaspersky**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'applicazione gestita selezionata:

- Nome applicazione

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al nome di un'applicazione Kaspersky.

  L'elenco contiene solo i nomi delle applicazioni con plug-in di gestione installati nella workstation dell'amministratore.

  Se non è selezionata alcuna applicazione, il criterio non verrà applicato.

- Versione applicazione

  Nel campo di immissione è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al numero versione di un'applicazione Kaspersky.

  Se non è specificato alcun numero di versione, il criterio non verrà applicato.

- Nome aggiornamento critico

  Nel campo di immissione è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al nome dell'applicazione o al numero del pacchetto di aggiornamento.

  Se il campo è vuoto, il criterio non verrà applicato.

- Stato applicazione

  Elenco a discesa da cui è possibile selezionare lo stato di un'applicazione (*Installata*, *Non installata*). Verranno inclusi nella selezione i dispositivi in cui è installata o non è installata l'applicazione specificata, in base allo stato selezionato.

- Selezionare il periodo dell'ultimo aggiornamento dei moduli

  È possibile utilizzare questa opzione per impostare un criterio per la ricerca dei dispositivi in base all'ora dell'ultimo aggiornamento dei moduli delle applicazioni installate in tali dispositivi.

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare l'intervallo di tempo (data e ora) durante il quale è stato eseguito l'ultimo aggiornamento dei moduli delle applicazioni installate in tali dispositivi.

  Se questa casella di controllo è deselezionata, il criterio non verrà applicato.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Il dispositivo è gestito tramite Administration Server

  Nell'elenco a discesa è possibile includere nella selezione i dispositivi gestiti tramite Kaspersky Security Center Linux:

  - **Sì**. L'applicazione include nella selezione i dispositivi gestiti tramite Kaspersky Security Center Linux.
  - **No**. L'applicazione include nella selezione i dispositivi non gestiti tramite Kaspersky Security Center Linux.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- L'applicazione di protezione è installata

  Nell'elenco a discesa è possibile includere nella selezione tutti i dispositivi in cui è installata l'applicazione di protezione:

  - **Sì**. L'applicazione include nella selezione tutti i dispositivi in cui è installata l'applicazione di protezione.
  - **No**. L'applicazione include nella selezione tutti i dispositivi in cui non è installata un'applicazione di protezione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

Nella sottosezione **Protezione anti-virus**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base allo stato della protezione:

- Data rilascio database

Se questa opzione è selezionata, è possibile eseguire la ricerca dei dispositivi client in base alla data di rilascio del database anti-virus. Nei campi di immissione è possibile impostare l'intervallo di tempo in base al quale eseguire la ricerca.

Per impostazione predefinita, questa opzione è disabilitata.

- **Conteggio record database**

  Se questa opzione è abilitata, è possibile eseguire la ricerca di dispositivi client in base al numero di record del database. Nei campi di immissione è possibile impostare i valori di soglia inferiore e superiore per i record del database anti-virus.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Ultima scansione**

  Se questa opzione è abilitata, è possibile eseguire la ricerca dei dispositivi client in base all'ora dell'ultima scansione malware. Nei campi di immissione è possibile specificare il periodo di tempo entro il quale è stata eseguita l'ultima scansione malware.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Minacce**

  Se questa opzione è abilitata, è possibile eseguire la ricerca di dispositivi client in base al numero di virus rilevati. Nei campi di immissione è possibile impostare i valori di soglia inferiore e superiore per il numero di virus trovati.

  Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Criptaggio**, è possibile configurare il criterio per l'inclusione dei dispositivi in una selezione in base all'algoritmo di criptaggio selezionato:

Algoritmo di criptaggio

Algoritmo di cifratura a blocchi AES (Advanced Encryption Standard). Nell'elenco a discesa è possibile selezionare le dimensioni della chiave di criptaggio (56 bit, 128 bit, 192 bit o 256 bit).

Valori disponibili: *AES56*, *AES128*, *AES192* e *AES256*.

La sottosezione **Componenti dell'applicazione** contiene un elenco dei componenti delle applicazioni per cui sono installati plug-in di gestione corrispondenti in Kaspersky Security Center Web Console.

Nella sottosezione **Componenti dell'applicazione**, è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base agli stati e ai numeri di versione dei componenti che fanno riferimento all'applicazione selezionata:

- **Stato**

Ricerca dei dispositivi in base allo stato dei componenti inviato da un'applicazione all'Administration Server. È possibile selezionare uno dei seguenti stati: *N/D, Arrestato*, *Sospeso*, *Avvio in corso*, *In esecuzione, Non riuscito, Non installato, Non supportato dalla licenza*. Se il componente selezionato dell'applicazione installata in un dispositivo gestito presenta lo stato specificato, il dispositivo viene incluso nella selezione dispositivi.

Stati inviati dalle applicazioni:

- *Arrestato* - Il componente è disabilitato e al momento non è in esecuzione.
- *Sospeso* - Il componente è sospeso, ad esempio dopo che l'utente ha sospeso la protezione nell'applicazione gestita.
- *Avvio in corso* - Il componente è attualmente in fase di inizializzazione.
- *In esecuzione* - Il componente è abilitato e correttamente in esecuzione.
- *Non riuscito* - Si è verificato un errore durante l'esecuzione del componente.
- *Non installato* - L'utente non ha selezionato il componente per l'installazione durante la configurazione dell'installazione personalizzata dell'applicazione.
- *Non supportato dalla licenza* - La licenza non copre il componente selezionato.

A differenza degli altri stati, lo stato *N/D* non viene inviato dalle applicazioni. Questa opzione indica che le applicazioni non dispongono di alcuna informazione sullo stato del componente selezionato. Ciò può ad esempio verificarsi quando il componente selezionato non appartiene ad alcuna delle applicazioni installate nel dispositivo o quando il dispositivo è spento.

- **Versione**

  Ricerca dei dispositivi in base al numero di versione del componente selezionato nell'elenco. È possibile digitare un numero di versione, ad esempio `3.4.1.0`, e quindi specificare se il componente selezionato deve avere una versione uguale, precedente o successiva. È anche possibile configurare la ricerca di tutte le versioni ad eccezione di quella specificata.

Tag

Nella sezione **Tag** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base alle parole chiave (tag) che sono state aggiunte in precedenza alle descrizioni dei dispositivi gestiti:

Applica se almeno uno dei tag specificati corrisponde

Se questa opzione è abilitata, i risultati di ricerca visualizzeranno i dispositivi con descrizioni contenenti almeno uno dei tag selezionati.

Se questa opzione è disabilitata, i risultati di ricerca visualizzeranno solo i dispositivi con descrizioni contenenti tutti i tag selezionati.

Per impostazione predefinita, questa opzione è disabilitata.

Per aggiungere tag al criterio, fare clic sul pulsante **Aggiungi** e selezionare i tag facendo clic sul campo di immissione **Tag**. Specificare se includere o escludere i dispositivi con i tag selezionati nella selezione di dispositivi.

- Deve essere incluso

  Se questa opzione è selezionata, i risultati di ricerca visualizzeranno i dispositivi le cui descrizioni contengono il tag selezionato. Per trovare i dispositivi è possibile utilizzare l'asterisco, che rappresenta qualsiasi stringa con qualsiasi numero di caratteri.

  Per impostazione predefinita, questa opzione è selezionata.

- Deve essere escluso

  Se questa opzione è selezionata, i risultati di ricerca visualizzeranno i dispositivi le cui descrizioni non contengono il tag selezionato. Per trovare i dispositivi è possibile utilizzare l'asterisco, che rappresenta qualsiasi stringa con qualsiasi numero di caratteri.

Utenti

Nella sezione **Utenti** è possibile impostare i criteri per l'inclusione dei dispositivi nella selezione in base agli account degli utenti che hanno eseguito l'accesso al sistema operativo.

- Ultimo utente che ha eseguito l'accesso al sistema

  Se questa opzione è abilitata, è possibile selezionare l'account utente per configurare il criterio. I risultati della ricerca includeranno i dispositivi in cui l'utente selezionato ha eseguito l'ultimo accesso al sistema.

- Utente che ha eseguito l'accesso al sistema almeno una volta

  Se questa opzione è abilitata, fare clic sul pulsante **Sfoglia** per specificare un account utente. I risultati della ricerca includeranno i dispositivi in cui l'utente specificato ha eseguito l'accesso al sistema almeno una volta.

Esportazione dell'elenco dei dispositivi da una selezione di dispositivi

Kaspersky Security Center Linux consente di salvare le informazioni sui dispositivi da una selezione di dispositivi ed esportarle in un file CSV o TXT.

Per esportare l'elenco dei dispositivi dalla selezione di dispositivi:

1. Aprire la tabella con i dispositivi dalla selezione di dispositivi.
2. Utilizzare uno dei seguenti metodi per selezionare i dispositivi che si desidera esportare:
   - Per selezionare dispositivi specifici, selezionare le caselle di controllo accanto ad essi.
   - Per selezionare tutti i dispositivi dalla pagina della tabella corrente, selezionare la casella di controllo nell'intestazione della tabella dei dispositivi, quindi selezionare la casella di controllo **Seleziona tutto nella pagina corrente**.
   - Per selezionare tutti i dispositivi dalla tabella, selezionare la casella di controllo nell'intestazione della tabella dei dispositivi, quindi selezionare la casella di controllo **Seleziona tutto**.

3. Fare clic sul pulsante **Esporta in CSV** o **Esporta in TXT**. Tutte le informazioni sui dispositivi selezionati inclusi nella tabella verranno esportate.

Si noti che se è stato applicato un criterio di filtraggio alla tabella dei dispositivi, solo i dati filtrati dalle colonne visualizzate verranno esportati.

Rimozione di dispositivi dai gruppi di amministrazione in una selezione

Durante l'utilizzo di una selezione dispositivi, è possibile rimuovere i dispositivi dai gruppi di amministrazione in questa selezione senza passare ai gruppi di amministrazione da cui devono essere rimossi i dispositivi.

Per rimuovere dispositivi dai gruppi di amministrazione:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Selezioni dispositivi** o **Individuazione e distribuzione** → **Selezioni dispositivi**.
2. Nell'elenco delle selezioni fare clic sul nome della selezione di dispositivi.

   La pagina mostra una tabella con le informazioni sui dispositivi inclusi nella selezione di dispositivi.
3. Selezionare i dispositivi che si desidera rimuovere, quindi fare clic su **Elimina**.

   I dispositivi selezionati verranno rimossi dai gruppi di amministrazione corrispondenti.

Tag dispositivo

Kaspersky Security Center Linux consente di eseguire il *tagging* dei dispositivi. Un tag è un valore di stringa che può essere utilizzato per raggruppare, descrivere o cercare i dispositivi. I tag assegnati ai dispositivi possono essere utilizzati per la creazione di selezioni, per il rilevamento dei dispositivi e per la distribuzione dei dispositivi tra i gruppi di amministrazione.

È possibile assegnare tag ai dispositivi in modalità manuale o automatica. Se si desidera assegnare tag a un singolo dispositivo, è possibile utilizzare l'assegnazione di tag manuale. L'assegnazione di tag automatica viene eseguita da Kaspersky Security Center Linux in uno dei seguenti modi:

- In conformità con le regole di assegnazione di tag specificate.
- Da un'applicazione.

Non è consigliabile utilizzare modi diversi di assegnazione di tag per assegnare lo stesso tag. Ad esempio, se il tag è assegnato dalla regola, non è consigliabile assegnarlo manualmente ai dispositivi.

Se i tag sono assegnati dalle regole, i tag vengono assegnati automaticamente ai dispositivi quando vengono soddisfatte le regole specificate. A ogni tag corrisponde una regola individuale. Le regole vengono applicate alle proprietà di rete del dispositivo, al sistema operativo, alle applicazioni installate nel dispositivo e ad altre proprietà del dispositivo. È ad esempio possibile impostare una regola che assegnerà il tag `[CentOS]` a tutti i dispositivi che eseguono il sistema operativo CentOS. Sarà quindi possibile utilizzare il tag durante la creazione di una selezione dispositivi. Questo consentirà di ordinare tutti i dispositivi CentOS e di assegnare loro un'attività.

Un tag viene rimosso automaticamente da un dispositivo nei seguenti casi:

- Quando il dispositivo smette di soddisfare le condizioni della regola per l'assegnazione del tag.
- Quando la regola per l'assegnazione del tag viene disabilitata o eliminata.

L'elenco dei tag e l'elenco delle regole in ciascun Administration Server sono indipendenti da tutti gli altri Administration Server, inclusi un Administration Server primario o gli Administration Server virtuali subordinati. Una regola viene applicata solo ai dispositivi nello stesso Administration Server in cui viene creata la regola.

Creazione di un tag dispositivo

Per creare un tag dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
2. Fare clic su **Aggiungi**.
   Verrà visualizzata una finestra per il nuovo tag.
3. Nel campo **Tag** immettere il nome del tag.
4. Fare clic su **Salva** per salvare le modifiche.

Il nuovo tag verrà visualizzato nell'elenco dei tag dispositivo.

Ridenominazione di un tag dispositivo

Per rinominare un tag dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
2. Fare clic sul nome del tag che si desidera rinominare.
   Verrà visualizzata una finestra delle proprietà del tag.
3. Nel campo **Tag** modificare il nome del tag.
4. Fare clic su **Salva** per salvare le modifiche.

Il tag aggiornato verrà visualizzato nell'elenco dei tag dispositivo.

Eliminazione di un tag dispositivo

È possibile eliminare solo i tag assegnati manualmente.

Per eliminare un tag assegnato manualmente a un dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
   Verrà visualizzato l'elenco di tag.

2. Selezionare il tag del dispositivo che si desidera eliminare.

3. Fare clic sul pulsante **Elimina**.

4. Nella finestra visualizzata fare clic su **Sì**.

   Il tag dispositivo verrà eliminato. Il tag eliminato viene rimosso automaticamente da tutti i dispositivi a cui è stato assegnato.

Quando si elimina un tag assegnato al dispositivo da una regola di assegnazione di tag automatica, la regola non viene eliminata e il tag verrà assegnato a un nuovo dispositivo quando il dispositivo soddisfa per la prima volta le condizioni della regola. Se si elimina una regola di assegnazione di tag automatica, il tag specificato nelle condizioni della regola verrà rimosso da tutti i dispositivi a cui è stato assegnato, ma non verrà eliminato dall'elenco di tag. Se necessario, è possibile eliminare manualmente il tag dall'elenco.

Il tag eliminato non viene rimosso automaticamente dal dispositivo se è assegnato al dispositivo da un'applicazione o da Network Agent. Per rimuovere il tag dal dispositivo, usare l'utilità klscflag.

Visualizzazione dei dispositivi a cui è assegnato un tag

Per visualizzare i dispositivi a cui è assegnato un tag:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.

2. Fare clic sul collegamento **Visualizza dispositivi** accanto al tag per cui si desidera visualizzare i dispositivi assegnati.

   L'elenco dei dispositivi visualizzato mostra solo i dispositivi a cui è assegnato il tag.

Per tornare all'elenco dei tag dispositivo, fare clic sul pulsante **Indietro** del browser.

Visualizzazione dei tag assegnati a un dispositivo

Per visualizzare i tag assegnati a un dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

2. Fare clic sul nome del dispositivo di cui si desidera visualizzare i tag.

3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Tag**.

   Verrà visualizzato l'elenco dei tag assegnati al dispositivo selezionato. Nella colonna **Tag assegnato** è possibile visualizzare come è stato assegnato il tag.

È possibile assegnare un altro tag al dispositivo o rimuovere un tag già assegnato. È inoltre possibile visualizzare tutti i tag dispositivo presenti in Administration Server.

È anche possibile visualizzare i tag assegnati a un dispositivo nella riga di comando utilizzando l'utilità klscflag.

Per visualizzare i tag assegnati a un dispositivo nella riga di comando, eseguire il seguente comando:

```
/opt/kaspersky/klnagent64/sbin/klscflag -ssvget -pv 1103/1.0.0.0 -s
KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -svt ARRAY_T -ss "|ss_type =
\"SS_PRODINFO\";"
```

Tagging manuale di un dispositivo

Per assegnare manualmente un tag a un dispositivo:

1. Visualizzare i tag assegnati al dispositivo a cui si desidera assegnare un altro tag.
2. Fare clic su **Aggiungi**.
3. Nella finestra visualizzata eseguire una delle seguenti operazioni:
   - Per creare e assegnare un nuovo tag, selezionare **Crea nuovo tag** e quindi specificare il nome del nuovo tag.
   - Per selezionare un tag esistente, selezionare **Assegna tag esistente** e quindi selezionare il tag desiderato nell'elenco a discesa.
4. Fare clic su **OK** per applicare le modifiche.
5. Fare clic su **Salva** per salvare le modifiche.

Il tag selezionato verrà assegnato al dispositivo.

Rimozione di un tag assegnato a un dispositivo

Per rimuovere un tag da un dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo di cui si desidera visualizzare i tag.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Tag**.
4. Selezionare la casella di controllo accanto al tag da rimuovere.
5. Nella parte superiore dell'elenco, fare clic sul pulsante **Annulla assegnazione tag**.
6. Nella finestra visualizzata fare clic su **Sì**.

Il tag viene rimosso dal dispositivo.

Il tag del dispositivo di cui è stata annullata l'assegnazione non viene eliminato. Se si desidera, è possibile eliminarlo manualmente.

Non è possibile rimuovere manualmente i tag assegnati al dispositivo dalle applicazioni o da Network Agent. Per rimuovere questi tag, utilizzare l'utilità klscflag.

Visualizzazione delle regole per il tagging automatico dei dispositivi

Per visualizzare le regole per il tagging automatico dei dispositivi:

Eseguire una delle seguenti operazioni:

- Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Regole di tagging automatico**.
- Nel menu principale, passare a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**, quindi fare clic sul collegamento **Configura regole di tagging automatico**.
- Visualizzare i tag assegnati a un dispositivo e fare clic sul pulsante **Impostazioni**.

Verrà visualizzato l'elenco delle regole per il tagging automatico dei dispositivi.

Modifica di una regola per il tagging automatico dei dispositivi

Per modificare una regola per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.
2. Fare clic sul nome della regola che si desidera modificare.
   Verrà visualizzata una finestra delle impostazioni della regola.
3. Modificare le proprietà generali della regola:
   a. Nel campo **Nome regola** modificare il nome della regola.
      Il nome non può superare i 256 caratteri.
   b. Eseguire una delle seguenti operazioni:
      - Abilitare la regola spostando l'interruttore su **Regola abilitata**.
      - Disabilitare la regola spostando l'interruttore su **Regola disabilitata**.
4. Eseguire una delle seguenti operazioni:
   - Se si desidera aggiungere una nuova condizione, fare clic sul pulsante **Aggiungi** e specificare le impostazioni della nuova condizione nella finestra visualizzata.

- Per modificare una condizione esistente, fare clic sul nome della condizione che si desidera modificare, quindi modificare le impostazioni della condizione.
- Per eliminare una condizione, selezionare la casella di controllo accanto al nome della condizione da eliminare, quindi fare clic su **Elimina**.

5. Fare clic su **OK** nella finestra delle impostazioni delle condizioni.
6. Fare clic su **Salva** per salvare le modifiche.

La regola modificata verrà visualizzata nell'elenco.

Creazione di una regola per il tagging automatico dei dispositivi

Per creare una regola per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.
2. Fare clic su **Aggiungi**.

   Verrà visualizzata una finestra delle impostazioni della nuova regola.
3. Configurare le proprietà generali della regola:

   a. Nel campo **Nome regola** immettere il nome della regola.

   Il nome non può superare i 256 caratteri.

   b. Eseguire una delle seguenti operazioni:

   - Abilitare la regola spostando l'interruttore su **Regola abilitata**.
   - Disabilitare la regola spostando l'interruttore su **Regola disabilitata**.

   c. Nel campo **Tag** immettere il nome del nuovo tag dispositivo o selezionare uno dei tag dispositivo esistenti dall'elenco.

   Il nome non può superare i 256 caratteri.
4. Nella sezione delle condizioni fare clic sul pulsante **Aggiungi** per aggiungere una nuova condizione.

   Verrà visualizzata una finestra delle impostazioni della nuova condizione.
5. Immettere il nome della condizione.

   Il nome non può superare i 256 caratteri. Il nome deve essere univoco all'interno di una regola.
6. Configurare l'attivazione della regola in base alle seguenti condizioni. È possibile selezionare più condizioni.

   - **Rete** - Proprietà di rete del dispositivo, ad esempio il nome DNS del dispositivo o l'inclusione del dispositivo in una subnet IP.

     Se per il database utilizzato per Kaspersky Security Center Linux sono impostate regole di confronto con distinzione tra maiuscole e minuscole, mantenere le maiuscole e le minuscole quando si specifica un nome DNS del dispositivo. In caso contrario, la regola di tagging automatico non funzionerà.

- **Applicazioni** - Presenza di Network Agent nel dispositivo, tipo di sistema operativo, versione e architettura.
- **Macchine virtuali** - Il dispositivo appartiene a un tipo specifico di macchina virtuale.
- **Registro delle applicazioni** - Presenza di applicazioni di vari produttori nel dispositivo.

7. Fare clic su **OK** per salvare le modifiche.

   Se necessario, è possibile impostare più condizioni per una singola regola. In questo caso, il tag verrà essere assegnato a un dispositivo se soddisfa almeno una condizione.

8. Fare clic su **Salva** per salvare le modifiche.

La nuova regola creata viene applicata ai dispositivi gestiti dall'Administration Server selezionato. Se le impostazioni di un dispositivo soddisfano le condizioni della regola, al dispositivo viene assegnato il tag.

Successivamente, la regola viene applicata nei seguenti casi:

- Automaticamente e periodicamente, a seconda del carico di lavoro del server
- Dopo aver modificato la regola
- Quando si esegue la regola manualmente
- Dopo che l'Administration Server rileva una modifica delle impostazioni di un dispositivo che soddisfa le condizioni della regola o delle impostazioni di un gruppo che contiene tale dispositivo

È possibile creare diverse regole di tagging. A un singolo dispositivo possono essere assegnati diversi tag se sono state create più regole di tagging e se vengono contemporaneamente soddisfatte le rispettive condizioni di tali regole. È possibile visualizzare l'elenco di tutti i tag assegnati nelle proprietà del dispositivo.

Esecuzione di regole per il tagging automatico dei dispositivi

Quando viene eseguita una regola, il tag specificato nelle proprietà di questa regola è assegnato ai dispositivi che soddisfano le condizioni specificate nelle proprietà della regola. È possibile eseguire solo regole attive.

Per eseguire le regole per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.
2. Selezionare le caselle di controllo accanto alle regole attive che si desidera eseguire.
3. Fare clic sul pulsante **Esegui regola**.

Le regole selezionate verranno eseguite.

Eliminazione di una regola per il tagging automatico dei dispositivi

Per eliminare una regola per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.

2. Selezionare la casella di controllo accanto alla regola che si desidera eliminare.

3. Fare clic su **Elimina**.

4. Nella finestra visualizzata fare di nuovo clic su **Elimina**.

La regola selezionata verrà eliminata. L'assegnazione del tag specificato nelle proprietà di questa regola viene annullata da tutti i dispositivi a cui il tag è stato assegnato.

Il tag del dispositivo di cui è stata annullata l'assegnazione non viene eliminato. Se si desidera, è possibile eliminarlo manualmente.

Gestione dei tag del dispositivo tramite l'utilità klscflag

Per assegnare un set di tag a un dispositivo, è necessario eseguire l'utilità klscflag nel dispositivo client a cui si desidera assegnare i tag.

L'utilità klscflag sovrascrive i tag esistenti assegnati al dispositivo. Ciò significa che è possibile aggiungere o rimuovere tag specificando il set di tag desiderato nel comando. L'utilità non dispone di comandi separati per aggiungere o rimuovere singoli tag. Invece, si modifica l'intero set di tag.

Quando si specificano i nomi dei tag in comandi come klscflag, si consiglia di utilizzare un approccio coerente per quanto riguarda le maiuscole e le minuscole, ad esempio usando solo lettere maiuscole. L'utilizzo di lettere maiuscole può aiutare a evitare potenziali problemi con i tag che differiscono solo per le maiuscole e le minuscole, a seconda della configurazione del DBMS.

Per assegnare uno o più tag al dispositivo utilizzando l'utilità klscflag:

1. Eseguire il prompt dei comandi in un account con privilegi di root, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella directory in cui è installato Network Agent. La directory di installazione predefinita è /opt/kaspersky/klnagent64/sbin/.

2. Immettere uno dei seguenti comandi:

   - Per assegnare un set di tag:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" TAG NAME 1 \",\" TAG NAME
     2 \",\" TAG NAME 3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     dove `[\" TAG NAME 1 \",\" TAG NAME 2 \",\" TAG NAME 3 \"]` è l'elenco dei tag che si desidera assegnare al dispositivo.

     Se si lasciano vuote le parentesi quadre, verranno rimossi tutti i tag dal dispositivo:

     ```
     /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
     KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type =
     \"SS_PRODINFO\";"
     ```

   - Per assegnare un nuovo tag a un set di tag esistente:

```
/opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NEW TAG NAME\",\"TAG NAME
1\",\"TAG NAME 2\",\"TAG NAME 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
```

dove `NEW TAG NAME` è il nome del tag che si desidera assegnare al dispositivo e `TAG NAME 1`, `TAG NAME 2`, `TAG NAME 3` sono i nomi dei tag già assegnati al dispositivo.

- Per rimuovere un tag specifico senza rimuovere gli altri tag già assegnati al dispositivo, eseguire il comando con il set di tag aggiornato.

  Ad esempio, se i tag correnti sono `TAG NAME 1`, `TAG NAME 2`, `TAG NAME 3` e si desidera rimuovere `TAG NAME 2`, eseguire il seguente comando:

  ```
  /opt/kaspersky/klnagent64/sbin/klscflag -ssvset -pv 1103/1.0.0.0 -s
  KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"TAG NAME 1\",\"TAG NAME 3\"]" -
  svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
  ```

3. Riavviare il servizio Network Agent.

   L'utilità klscflag assegna i tag specificati al dispositivo.

4. Se si desidera accertarsi che l'utilità klscflag abbia assegnato correttamente i tag specificati, visualizzare i tag assegnati al dispositivo.

In alternativa, è possibile assegnare i tag del dispositivo manualmente.

Criptaggio e protezione dei dati

Il criptaggio dei dati riduce il rischio di perdita involontaria di dati sensibili e aziendali in caso di furto o smarrimento del laptop o del disco rigido. Inoltre, il criptaggio dei dati consente di impedire l'accesso da parte di utenti e applicazioni non autorizzati.

È possibile utilizzare la funzionalità di criptaggio dei dati se la rete include dispositivi gestiti basati su Windows con Kaspersky Endpoint Security for Windows installato. In questo caso, nei dispositivi in cui viene eseguito un sistema operativo Windows, è possibile gestire i seguenti tipi di criptaggio:

- Crittografia unità BitLocker
- Criptaggio disco Kaspersky

Utilizzando questi componenti di Kaspersky Endpoint Security for Windows è ad esempio possibile abilitare o disabilitare il criptaggio, visualizzare l'elenco delle unità criptate o generare e visualizzare rapporti sul criptaggio.

Per configurare il criptaggio, definire il criterio di Kaspersky Endpoint Security for Windows in Kaspersky Security Center Linux. Kaspersky Endpoint Security for Windows esegue il criptaggio e il decriptaggio in base al criterio attivo. Per istruzioni dettagliate su come configurare le regole e una descrizione delle funzionalità di criptaggio, consultare la Guida di Kaspersky Endpoint Security for Windows.

La gestione del criptaggio per una gerarchia di Administration Server non è attualmente disponibile in Web Console. Utilizzare l'Administration Server primario per gestire i dispositivi criptati.

È possibile mostrare o nascondere alcuni degli elementi dell'interfaccia relativi alla funzionalità di gestione del criptaggio utilizzando le impostazioni dell'interfaccia utente.

Visualizzazione dell'elenco delle unità criptate

In Kaspersky Security Center Linux, è possibile visualizzare i dettagli sulle unità criptate e sui dispositivi criptati a livello di unità. Una volta decriptate le informazioni in un'unità, l'unità viene automaticamente rimossa dall'elenco.

Per visualizzare l'elenco delle unità criptate:

Nel menu principale accedere a **Operazioni** → **Criptaggio e protezione dei dati** → **Unità criptate**.

Se la sezione non è visibile nel menu, significa che è nascosta. Nelle impostazioni dell'interfaccia utente. abilitare l'opzione **Mostra Criptaggio e protezione dei dati** per visualizzare la sezione.

È possibile esportare l'elenco delle unità criptate in un file CSV o TXT. A tale scopo, fare clic sul pulsante **Esporta in CSV** o **Esporta in TXT**.

Visualizzazione dell'elenco degli eventi di criptaggio

Durante l'esecuzione delle attività di criptaggio o decriptaggio dei dati nei dispositivi, Kaspersky Endpoint Security for Windows invia a Kaspersky Security Center Linux informazioni sui seguenti tipi di eventi:

- Impossibile criptare o decriptare un file o creare un archivio criptato perché lo spazio sul disco rigido non è sufficiente.
- Impossibile criptare o decriptare un file o creare un archivio criptato a causa dei problemi di licenza.
- Impossibile criptare o decriptare un file o creare un archivio criptato a causa di diritti di accesso insufficienti.
- All'applicazione è stato negato l'accesso a un file criptato.
- Errori sconosciuti.

Per visualizzare un elenco degli eventi che si sono verificati durante il criptaggio dei dati nei dispositivi:

Nel menu principale accedere a **Operazioni** → **Criptaggio e protezione dei dati** → **Eventi di criptaggio**.

Se la sezione non è visibile nel menu, significa che è nascosta. Nelle impostazioni dell'interfaccia utente. abilitare l'opzione **Mostra Criptaggio e protezione dei dati** per visualizzare la sezione.

È possibile esportare l'elenco delle unità criptate in un file CSV o TXT. A tale scopo, fare clic sul pulsante **Esporta in CSV** o **Esporta in TXT**.

In alternativa è possibile esaminare l'elenco degli eventi di criptaggio per ogni dispositivo gestito.

Per visualizzare gli eventi di criptaggio di un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome di un dispositivo gestito.
3. Nella scheda **Generale**, passare alla sezione **Protezione**.

4. Fare clic sul collegamento **Visualizza errori di criptaggio dei dati**.

Creazione e visualizzazione di rapporti sul criptaggio

È possibile generare i seguenti rapporti:

- Rapporto sullo stato di criptaggio dei dispositivi gestiti. Questo rapporto include informazioni dettagliate sul criptaggio dei dati di vari dispositivi gestiti. Il rapporto mostra ad esempio il numero di dispositivi a cui si applica il criterio con regole di criptaggio configurate. È inoltre possibile scoprire, ad esempio, quanti dispositivi devono essere riavviati. Il rapporto contiene inoltre le informazioni sulla tecnologia di criptaggio e sull'algoritmo di ogni dispositivo.

- Rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa. Questo rapporto contiene informazioni simili a quelle del rapporto sullo stato di criptaggio dei dispositivi gestiti, ma fornisce solo i dati relativi a dispositivi di archiviazione di massa e unità rimovibili.

- Rapporto sui diritti di accesso alle unità criptate. Questo rapporto mostra quali account utente hanno accesso alle unità criptate.

- Rapporto sugli errori di criptaggio dei file. Questo rapporto contiene informazioni sugli errori che si sono verificati durante l'esecuzione delle attività di criptaggio o decriptaggio dei dati nei dispositivi.

- Rapporto sul blocco dell'accesso ai file criptati. Questo rapporto contiene informazioni sul blocco dell'accesso delle applicazioni ai file criptati. Questo rapporto è utile se un utente o un'applicazione non autorizzati tentano di accedere a unità o file criptati.

È possibile generare qualsiasi rapporto nella sezione **Monitoraggio e generazione dei rapporti → Rapporti**. In alternativa, nella sezione **Operazioni → Criptaggio e protezione dei dati**, è possibile generare i seguenti rapporti di criptaggio:

- Rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa

- Rapporto sui diritti di accesso alle unità criptate

- Rapporto sugli errori di criptaggio dei file

*Per generare un rapporto sul criptaggio nella sezione **Criptaggio e protezione dei dati**:*

1. Assicurarsi di avere abilitato l'opzione **Mostra Criptaggio e protezione dei dati** in Opzioni di interfaccia.

2. Nelle proprietà del criterio aprire la scheda **Configurazione eventi**.

3. Nella sezione **Critico**, fare clic su **Aggiungi evento** e selezionare la casella di controllo accanto all'evento *Errore durante l'applicazione delle regole di criptaggio/decriptaggio dei file*.

4. Fare clic su **OK**.

5. Nel menu principale accedere a **Operazioni → Criptaggio e protezione dei dati**.

6. Aprire una delle seguenti sezioni:

   - **Unità criptate** genera il rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa o il rapporto sui diritti di accesso alle unità criptate.

- **Eventi di criptaggio** genera il rapporto sugli errori di criptaggio dei file.

7. Fare clic sul nome del rapporto che si desidera generare.

Verrà avviata la generazione del rapporto.

Concedere l'accesso a un'unità criptata in modalità offline

Un utente può richiedere l'accesso a un dispositivo criptato, ad esempio quando Kaspersky Endpoint Security for Windows non è installato nel dispositivo gestito. Dopo aver ricevuto la richiesta, è possibile creare un file della chiave di accesso e inviarlo all'utente. Tutti i casi di utilizzo e le istruzioni dettagliate sono disponibili nella Guida di Kaspersky Endpoint Security for Windows.

Per concedere l'accesso a un'unità criptata in modalità offline:

1. Ottenere un file della richiesta di accesso da un utente (un file con estensione FDERTC). Seguire le istruzioni contenute nella Guida di Kaspersky Endpoint Security for Windows per generare il file in Kaspersky Endpoint Security for Windows.

2. Nel menu principale accedere a **Operazioni** → **Criptaggio e protezione dei dati** → **Unità criptate**.

   Verrà visualizzato un elenco di unità criptate.

3. Selezionare l'unità a cui l'utente ha richiesto l'accesso.

4. Fare clic sul pulsante **Concedi l'accesso al dispositivo in modalità offline**.

5. Nella finestra visualizzata, selezionare il plug-in Kaspersky Endpoint Security for Windows.

6. Seguire le istruzioni fornite nella Guida di Kaspersky Endpoint Security for Windows (consultare le istruzioni per Kaspersky Security Center Web Console alla fine della sezione).

Successivamente l'utente applica il file ricevuto per accedere all'unità criptata e leggere i dati archiviati nell'unità.

Modifica di Administration Server per i dispositivi client

È possibile modificare l'Administration Server in uno diverso per dispositivi client specifici. A tale scopo, utilizzare l'attività *Cambia Administration Server*.

Per sostituire l'Administration Server che gestisce i dispositivi client con un altro server:

1. Eseguire la connessione all'Administration Server che gestisce i dispositivi.

2. Creare l'attività di modifica dell'Administration Server.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata. Nella finestra **Nuova attività** della Creazione guidata nuova attività, selezionare l'applicazione **Kaspersky Security Center 15** e il tipo di attività **Cambia Administration Server**. Successivamente, specificare i dispositivi per i quali si desidera modificare l'Administration Server:

   - **Assegna attività a un gruppo di amministrazione**

L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

- **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**

  È possibile specificare nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

  Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

- **Assegna attività a una selezione dispositivi**

  L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

3. Eseguire l'attività creata.

Dopo il completamento dell'attività, i dispositivi client per cui è stata creata passano sotto la gestione dell'Administration Server specificato nelle impostazioni dell'attività.

Se l'Administration Server supporta il criptaggio e la protezione dei dati e si sta creando un'attività Cambia Administration Server, viene visualizzato un avviso. L'avviso indica che, se nei dispositivi sono contenuti dati criptati, quando il nuovo server inizia a gestire i dispositivi, gli utenti saranno in grado di accedere solo ai dati criptati che hanno utilizzato in precedenza. In nessun altro caso sarà possibile accedere ai dati criptati. Per descrizioni dettagliate degli scenari in cui non è possibile accedere ai dati criptati, fare riferimento alla Guida di Kaspersky Endpoint Security for Windows.

Spostamento dei dispositivi connessi ad Administration Server tramite gateway di connessione a un altro Administration Server

È possibile spostare i dispositivi connessi ad Administration Server tramite i gateway di connessione in un altro Administration Server. Questa operazione potrebbe ad esempio essere necessaria se si installa un'altra versione di Administration Server e non si desidera reinstallare Network Agent nei dispositivi, poiché ciò potrebbe richiedere molto tempo.

I comandi descritti nelle istruzioni devono essere eseguiti nei dispositivi client con un account con diritti di amministratore.

Per spostare un dispositivo connesso tramite il gateway di connessione in un altro Administration Server:

1. Eseguire l'utilità klmover con `-address <indirizzo server>` per passare al nuovo Administration Server.
2. Eseguire il comando `klnagchk -nagwait -tl 4`.
3. Eseguire i seguenti comandi per impostare un nuovo gateway di connessione:
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "gateway_ip_or_name" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Qui `gateway_ip_or_name` è l'indirizzo del gateway di connessione accessibile da Internet.
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` è il numero della porta TCP in ascolto del gateway di connessione.
4. Eseguire il comando `klnagchk -restart -tl 4` per avviare il servizio Network Agent.

Il dispositivo viene spostato nel nuovo Administration Server e connesso tramite il nuovo gateway connesso.

Visualizzazione e configurazione delle azioni per i dispositivi inattivi

È possibile ottenere notifiche relative ai dispositivi client all'interno di un gruppo che risultano inattivi. È anche possibile eliminare automaticamente tali dispositivi.

Per visualizzare o configurare le azioni eseguite quando i dispositivi nel gruppo risultano inattivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Fare clic sul nome del gruppo di amministrazione desiderato.

   Verrà visualizzata la finestra delle proprietà dal gruppo di amministrazione.
3. Nella finestra delle proprietà passare alla scheda **Impostazioni**.
4. Nella sezione **Ereditarietà** abilitare o disabilitare le seguenti opzioni:
   - **Eredita da gruppo padre**

     Le impostazioni di questa sezione saranno ereditate dal gruppo padre di cui fa parte il dispositivo client. Se questa opzione è abilitata, le impostazioni in **Attività dei dispositivi nella rete** sono bloccate dalle modifiche.

     Questa opzione è disponibile solo se il gruppo di amministrazione ha un gruppo padre.

     Per impostazione predefinita, questa opzione è abilitata.
   - **Forza ereditarietà delle impostazioni nei gruppi figlio**

I valori delle impostazioni vengono distribuiti ai gruppi figlio, ma nelle proprietà dei gruppi figlio tali impostazioni sono bloccate.

Per impostazione predefinita, questa opzione è disabilitata.

5. Nella sezione **Attività dei dispositivi** abilitare o disabilitare le seguenti opzioni:

- Avvisa l'amministratore se il dispositivo è inattivo da più di (giorni)

  Se questa opzione è abilitata, l'amministratore riceve le notifiche sui dispositivi inattivi. È possibile specificare l'intervallo di tempo al termine del quale verrà creato l'evento **Il dispositivo risulta inattivo nella rete da molto tempo**. L'intervallo di tempo predefinito è 7 giorni.

  Per impostazione predefinita, questa opzione è abilitata.

- Rimuovi il dispositivo dal gruppo se è inattivo da più di (giorni)

  Se questa opzione è abilitata, è possibile specificare l'intervallo di tempo al termine del quale il dispositivo viene rimosso automaticamente dal gruppo. L'intervallo di tempo predefinito è 60 giorni.

  Per impostazione predefinita, questa opzione è abilitata.

6. Fare clic su **Salva**.

Le modifiche verranno salvate e applicate.

Invio di messaggi agli utenti dei dispositivi

Per inviare un messaggio agli utenti dei dispositivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.
3. Nell'elenco a discesa **Tipo di attività**, selezionare **Invia messaggio all'utente**.
4. Selezionare un'opzione per specificare il gruppo di amministrazione, la selezione dispositivi o i dispositivi a cui si applica l'attività.
5. Eseguire l'attività creata.

Al termine dell'attività, il messaggio creato verrà inviato agli utenti dei dispositivi selezionati. L'attività **Invia messaggio all'utente** è disponibile solo per i dispositivi che eseguono Windows.

Accensione, spegnimento e riavvio dei dispositivi client in remoto

Kaspersky Security Center Linux consente di gestire in remoto i dispositivi client accendendoli, spegnendoli o riavviandoli.

Per gestire in remoto i dispositivi client:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.
3. Nell'elenco a discesa **Tipo di attività** selezionare **Gestisci dispositivi**.
4. Selezionare un'opzione per specificare il gruppo di amministrazione, la selezione dispositivi o i dispositivi a cui si applica l'attività.
5. Selezionare il comando (accensione, spegnimento o riavvio).
6. Se necessario, configurare le seguenti impostazioni per i comandi di spegnimento e riavvio:

   - Attivare l'interruttore **Richiedi conferma all'utente** per specificare il messaggio di richiesta dell'utente e gli intervalli di tempo dopo i quali si desidera ripetere la richiesta e riavviare o spegnere i dispositivi.
   - Selezionare la casella di controllo **Tempo di attesa prima della chiusura forzata delle applicazioni nelle sessioni bloccate (min.)** e specificare l'ora.

   Queste impostazioni sono applicabili solo ai dispositivi client Windows. I dispositivi Linux verranno riavviati o spenti subito dopo il completamento dell'attività.
7. Eseguire l'attività creata.

Al termine dell'attività, il comando (accensione, spegnimento o riavvio) verrà eseguito sui dispositivi selezionati.

Gestione dei gruppi di amministrazione

Questa sezione contiene informazioni su come gestire i gruppi di amministrazione.

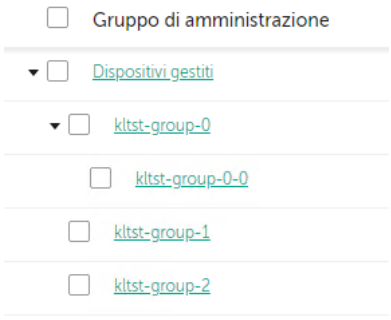
È possibile eseguire le seguenti azioni sui gruppi di amministrazione:

- Aggiungere un numero illimitato di gruppi nidificati a qualsiasi livello della gerarchia dei gruppi di amministrazione.
- Aggiungere dispositivi ai gruppi di amministrazione.
- Modificare la gerarchia dei gruppi di amministrazione spostando singoli dispositivi e interi gruppi in altri gruppi.
- Rimuovere gruppi nidificati e dispositivi dai gruppi di amministrazione.
- Aggiungere Administration Server secondari e virtuali ai gruppi di amministrazione.
- Spostare dispositivi dai gruppi di amministrazione di un Administration Server a quelli di un altro server.
- Definire le applicazioni Kaspersky da installare automaticamente nei dispositivi inclusi in un gruppo.

È possibile eseguire queste azioni solo se si dispone dell'autorizzazione **Modifica** nell'area **Gestione dei gruppi di amministrazione** per i gruppi di amministrazione che si desidera gestire (o per l'Administration Server a cui appartengono questi gruppi).

Creazione dei gruppi di amministrazione

Subito dopo l'installazione di Kaspersky Security Center, la gerarchia dei gruppi di amministrazione contiene un solo gruppo di amministrazione, denominato **Dispositivi gestiti**. Durante la creazione di una gerarchia di gruppi di amministrazione, è possibile aggiungere dispositivi e macchine virtuali al gruppo **Dispositivi gestiti**, nonché aggiungere gruppi nidificati (vedere la figura di seguito).



Visualizzazione della gerarchia di gruppi di amministrazione

Per creare un gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nella struttura di gruppi di amministrazione selezionare il gruppo di amministrazione che deve includere il nuovo gruppo di amministrazione.
3. Fare clic sul pulsante **Aggiungi**.

4. Nella finestra **Nome del nuovo gruppo di amministrazione** visualizzata immettere un nome per il gruppo, quindi fare clic sul pulsante **Aggiungi**.

Un nuovo gruppo di amministrazione con il nome specificato viene visualizzato nella gerarchia dei gruppi di amministrazione.

Per creare una struttura di gruppi di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Fare clic sul pulsante **Importa**.

Verrà avviata la Creazione guidata nuova struttura dei gruppi di amministrazione. Seguire le istruzioni della procedura guidata.

Installazione automatica delle applicazioni nei dispositivi di un gruppo di amministrazione

È possibile specificare i pacchetti di installazione da utilizzare per l'installazione remota delle applicazioni Kaspersky nei dispositivi client in un gruppo di amministrazione.

Per configurare l'installazione automatica delle applicazioni nei dispositivi di un gruppo di amministrazione:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Gerarchia dei gruppi** e fare clic sul nome del gruppo di amministrazione richiesto.
2. Nella finestra delle proprietà visualizzata passare alla scheda **Installazione automatica**.
3. Selezionare i pacchetti di installazione delle applicazioni da installare nei dispositivi, quindi fare clic sul pulsante **Salva**.

   Se si selezionano più pacchetti di installazione della stessa applicazione che differiscono solo nella versione, verrà salvato il pacchetto di installazione con la versione più recente.

Dopo aver selezionato i pacchetti di installazione, per ciascuna applicazione viene creato un gruppo di attività per l'installazione delle applicazioni nei dispositivi nel gruppo di amministrazione. Queste attività vengono eseguite nei dispositivi client subito dopo essere stati aggiunti al gruppo di amministrazione.

Spostamento di gruppi di amministrazione

È possibile spostare i gruppi di amministrazione nidificati all'interno della gerarchia dei gruppi.

Un gruppo di amministrazione viene spostato con tutti i gruppi nidificati, gli Administration Server secondari, i dispositivi, i criteri e le attività di gruppo. Il sistema applica al gruppo tutte le impostazioni che corrispondono alla nuova posizione nella gerarchia dei gruppi di amministrazione.

Il nome del gruppo deve essere univoco all'interno del livello della gerarchia. Se un gruppo con lo stesso nome esiste già nella cartella in cui si sposta il gruppo di amministrazione, è necessario cambiare il nome di quest'ultimo. Se non si modifica il nome del gruppo spostato, dopo lo spostamento al nome viene aggiunto un indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Non è possibile rinominare e spostare il gruppo **Dispositivi gestiti**.

Per spostare un gruppo di amministrazione a un altro livello della gerarchia dei gruppi di amministrazione:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Gerarchia dei gruppi**, quindi selezionare la casella di controllo accanto al gruppo di amministrazione da spostare.

2. Fare clic sul pulsante **Sposta** sulla barra degli strumenti.

3. Nella finestra visualizzata, selezionare dove spostare il gruppo di amministrazione e fare clic sul pulsante **Sposta**.

La finestra viene chiusa e il gruppo di amministrazione viene spostato a un altro livello della gerarchia dei gruppi.

Eliminazione di gruppi di amministrazione

Se si elimina un gruppo di amministrazione che contiene Administration Server secondari, gruppi nidificati, dispositivi client, attività di gruppo o criteri creati per questo gruppo, verranno eliminati anche tutti gli altri.

Prima di eliminare un gruppo di amministrazione, è necessario rimuovere da tale gruppo tutti gli Administration Server secondari, i gruppi nidificati e i dispositivi client.

Per eliminare un gruppo di amministrazione:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Gerarchia dei gruppi**, quindi selezionare la casella di controllo accanto al gruppo di amministrazione da eliminare.

2. Fare clic sul pulsante **Elimina** sulla barra degli strumenti.

Il gruppo di amministrazione viene eliminato.

Distribuzione delle applicazioni Kaspersky

In questa sezione viene descritta la distribuzione delle applicazioni Kaspersky nei dispositivi client dell'organizzazione tramite Kaspersky Security Center Web Console.

Scenario: Distribuzione delle applicazioni Kaspersky

In questo scenario viene descritto come distribuire le applicazioni Kaspersky tramite Kaspersky Security Center Web Console. È possibile utilizzare l'Avvio rapido guidato e la Distribuzione guidata della protezione oppure completare manualmente tutti i passaggi necessari.

Le seguenti applicazioni sono disponibili per la distribuzione tramite Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

Passaggi

La distribuzione delle applicazioni Kaspersky prevede diversi passaggi:

1. **Download del plug-in Web di gestione per l'applicazione**

   Questo passaggio viene gestito dall'Avvio rapido guidato. Se si sceglie di non eseguire la procedura guidata, scaricare i plug-in manualmente.

2. **Download e creazione dei pacchetti di installazione**

   Questo passaggio viene gestito dall'Avvio rapido guidato.

   L'Avvio rapido guidato consente di scaricare il pacchetto di installazione con il plug-in Web di gestione. Se non è stata selezionata questa opzione durante l'esecuzione della procedura guidata o se la procedura guidata non è stata eseguita affatto, è necessario scaricare il pacchetto manualmente.

   Se non è possibile installare le applicazioni Kaspersky tramite Kaspersky Security Center Linux in alcuni dispositivi, ad esempio nei dispositivi dei dipendenti remoti, è possibile creare pacchetti di installazione indipendenti per le applicazioni. Se si utilizzano pacchetti indipendenti per installare le applicazioni Kaspersky, non è necessario creare ed eseguire un'attività di installazione remota, né creare e configurare attività per Kaspersky Endpoint Security for Windows.

   In alternativa, è possibile scaricare i pacchetti di distribuzione per Network Agent e le applicazioni di protezione dal sito Web di Kaspersky. Se l'installazione remota delle applicazioni non è possibile per qualche motivo, è possibile utilizzare i pacchetti di distribuzione scaricati per installare le applicazioni in locale.

3. **Creazione, configurazione ed esecuzione dell'attività di installazione remota**

   Questo passaggio fa parte della Distribuzione guidata della protezione. Se si sceglie di non eseguire la Distribuzione guidata della protezione, è necessario creare questa attività manualmente e configurarla manualmente.

   È inoltre possibile creare manualmente diverse attività di installazione remota per diversi gruppi di amministrazione o diverse selezioni dispositivi. È possibile distribuire versioni differenti di un'applicazione in queste attività.

   Assicurarsi che vengano rilevati tutti i dispositivi nella rete, quindi eseguire l'attività (o le attività) di installazione remota.

Se si desidera installare Network Agent nei dispositivi con sistema operativo SUSE Linux Enterprise Server 15, installare il pacchetto insserv-compat prima di configurare Network Agent.

4. **Creazione e configurazione delle attività**

   È necessario configurare l'attività *Aggiornamento* di Kaspersky Endpoint Security.

   Questo passaggio fa parte dell'avvio rapido guidato: l'attività verrà creata e configurata automaticamente con le impostazioni predefinite. Se la procedura guidata non è stata eseguita, è necessario creare questa attività manualmente e configurarla manualmente. Se si utilizza l'Avvio rapido guidato, assicurarsi che la pianificazione dell'attività soddisfi i requisiti. Per impostazione predefinita, l'avvio pianificato dell'attività è impostato su **Manualmente**, ma è consigliabile scegliere un'altra opzione.

5. **Creazione dei criteri in corso**

   Creare il criterio per Kaspersky Endpoint Security manualmente o tramite l'Avvio rapido guidato. È possibile utilizzare le impostazioni predefinite del criterio, nonché modificare le impostazioni predefinite del criterio in base alle esigenze in qualsiasi momento.

6. **Verifica dei risultati**

   Assicurarsi che la distribuzione sia stata completata correttamente: sono disponibili criteri e attività per ciascuna applicazione e tali applicazioni sono installate nei dispositivi gestiti.

Risultati

Il completamento dello scenario dà i seguenti risultati:

- Vengono creati tutti i criteri e le attività richiesti per le applicazioni selezionate.
- Le pianificazioni delle attività sono configurate in base alle esigenze.
- Le applicazioni selezionate sono distribuite, o pianificate per essere distribuite, nei dispositivi client selezionati.

Aggiunta dei plug-in di gestione per le applicazioni Kaspersky

Per distribuire un'applicazione Kaspersky, come Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security for Windows, è necessario aggiungere e installare il plug-in Web di gestione per l'applicazione.

Per scaricare un plug-in Web di gestione per un'applicazione Kaspersky:

1. Nel menu principale accedere a **Impostazioni** → **Plug-in Web**.
2. Nella finestra visualizzata fare clic sul pulsante **Aggiungi**.

   Verrà visualizzato l'elenco dei plug-in disponibili.
3. Nell'elenco dei plug-in disponibili selezionare il plug-in che si desidera scaricare (ad esempio, Kaspersky Endpoint Security for Linux) facendo clic sul relativo nome.

   Verrà visualizzata una pagina di descrizione del plug-in.
4. Nella pagina di descrizione del plug-in fare clic su **Installa plug-in**.
5. Al termine dell'installazione, fare clic su **OK**.

Il plug-in Web di gestione verrà scaricato con la configurazione predefinita e visualizzato nell'elenco dei plug-in Web di gestione.

È possibile aggiungere plug-in e aggiornare i plug-in scaricati da un file. È possibile scaricare i plug-in Web di gestione dal sito Web di Kaspersky.

Per scaricare o aggiornare il plug-in Web di gestione da un file:

1. Nel menu principale accedere a **Impostazioni** → **Plug-in Web**.
2. Specificare il file del plug-in e la firma del file:
   - Fare clic su **Aggiungi da file** per scaricare un plug-in da un file.
   - Fare clic su **Aggiorna da file** per scaricare l'aggiornamento di un plug-in da un file.
3. Specificare il file e la firma del file.
4. Scaricare i file specificati.

Il plug-in Web di gestione verrà scaricato dal file e visualizzato nell'elenco dei plug-in di gestione.

Download e creazione dei pacchetti di installazione per le applicazioni Kaspersky

È possibile creare pacchetti di installazione per le applicazioni Kaspersky dai server Web di Kaspersky se l'Administration Server dispone di accesso a Internet.

Per scaricare e creare il pacchetto di installazione per l'applicazione Kaspersky:

1. Eseguire una delle seguenti operazioni:
   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.
   - Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

   È anche possibile visualizzare le notifiche relative ai nuovi pacchetti per le applicazioni Kaspersky nell'elenco delle notifiche sullo schermo. Se sono presenti notifiche relative a un nuovo pacchetto, è possibile fare clic sul collegamento accanto alla notifica e passare all'elenco dei pacchetti di installazione disponibili.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.
2. Fare clic su **Aggiungi**.

   Viene avviata la Creazione guidata nuovo pacchetto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Selezionare **Crea pacchetto di installazione per un'applicazione Kaspersky**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili sui server Web di Kaspersky. L'elenco contiene i pacchetti di installazione solo per le applicazioni compatibili con la versione corrente di Kaspersky Security Center Linux.

4. Fare clic sul nome di un pacchetto di installazione, ad esempio Kaspersky Endpoint Security for Linux.

   Verrà visualizzata una finestra con le informazioni sul pacchetto di installazione.

   È possibile scaricare e utilizzare un pacchetto di installazione che includa strumenti di criptaggio che implementano la crittografia avanzata, se conforme alle leggi e ai regolamenti vigenti. Per scaricare il pacchetto di installazione di Kaspersky Endpoint Security for Windows valido per le esigenze aziendali, consultare le normative del paese in cui si trovano i dispositivi client dell'organizzazione.

5. Leggere le informazioni e fare clic sul pulsante **Scarica e crea pacchetto di installazione**.

   Se un pacchetto di distribuzione non può essere convertito in un pacchetto di installazione, viene visualizzato il pulsante **Scarica pacchetto di distribuzione** anziché **Scarica e crea pacchetto di installazione**.

   Verrà avviato il download del pacchetto di installazione in Administration Server. È possibile chiudere la finestra della procedura guidata o procedere al passaggio successivo della procedura. Se si chiude la finestra della procedura guidata, il processo di download continuerà in background.

   Se si desidera tenere traccia del processo di download di un pacchetto di installazione:

   a. Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione** → **In corso ()**.

   b. Tenere traccia dello stato di avanzamento dell'operazione nella colonna **Stato di avanzamento del download** e nella colonna **Stato del download** della tabella.

   Al termine del processo, il pacchetto di installazione viene aggiunto all'elenco nella scheda **Download eseguito**. Se il processo di download si interrompe e lo stato del download passa a **Accetta Contratto di licenza con l'utente finale**, fare clic sul nome del pacchetto di installazione, quindi procedere al passaggio successivo della procedura.

   Se la dimensione dei dati contenuti nel pacchetto di distribuzione selezionato supera il limite corrente, viene visualizzato un messaggio di errore. È possibile modificare il valore limite, quindi procedere con la creazione del pacchetto di installazione.

6. Per alcune applicazioni Kaspersky, durante il processo di download viene visualizzato il pulsante **Mostra Contratto di licenza con l'utente finale**. Se viene visualizzato, procedere come segue:

   a. Fare clic sul pulsante **Mostra Contratto di licenza con l'utente finale** per leggere il Contratto di licenza con l'utente finale (EULA).

   b. Leggere il Contratto di licenza con l'utente finale visualizzato, quindi fare clic su **Accetta**.

      Dopo aver accettato il Contratto di licenza con l'utente finale, il download prosegue. Se si fa clic su **Rifiuta**, il download viene interrotto.

7. Al termine del download, fare clic sul pulsante **Chiudi**.

Il pacchetto di installazione selezionato verrà scaricato nella cartella condivisa di Administration Server, nella sottocartella Pacchetti. Dopo il download, il pacchetto di installazione viene visualizzato nell'elenco dei pacchetti di installazione.

Creazione di pacchetti di installazione da un file

È possibile utilizzare pacchetti di installazione personalizzati per effettuare le seguenti operazioni:

- Installare qualsiasi applicazione (come un editor di testo) in un dispositivo client, ad esempio mediante un'attività.
- Per creare un pacchetto di installazione indipendente.

Un pacchetto di installazione personalizzato è una cartella con un set di file. L'origine per creare un pacchetto di installazione personalizzato è un *file di archivio*. Il file di archivio contiene uno o più file che devono essere inclusi nel pacchetto di installazione personalizzato.

Durante la creazione di un pacchetto di installazione personalizzato, è possibile specificare i parametri della riga di comando, ad esempio per installare l'applicazione in modalità automatica.

Per creare un pacchetto di installazione personalizzato:

1. Eseguire una delle seguenti operazioni:
   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.
   - Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.
2. Fare clic su **Aggiungi**.

   Viene avviata la Creazione guidata nuovo pacchetto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Selezionare **Crea pacchetto di installazione da un file**.
4. Specificare il nome del pacchetto e fare clic sul pulsante **Sfoglia**.
5. Nella finestra visualizzata scegliere un file di archivio presente nei dischi disponibili.

   È possibile caricare un file di archivio ZIP, CAB, TAR o TAR.GZ. Non è possibile creare un pacchetto di installazione da un file SFX (archivio autoestraente).

   Verrà avviato il caricamento del file in Administration Server.
6. Se è stato specificato un file di un'applicazione Kaspersky, potrebbe essere richiesto di leggere e accettare il Contratto di licenza con l'utente finale (EULA) per l'applicazione. Per continuare, è necessario accettare il Contratto di licenza con l'utente finale. Selezionare l'opzione **Accetta i termini e le condizioni del presente Contratto di licenza con l'utente finale** solo se sono stati letti, compresi e accettati integralmente i termini del Contratto di licenza con l'utente finale.

   Potrebbe inoltre essere richiesto di leggere e accettare l'Informativa sulla privacy. Per continuare, è necessario accettare l'Informativa sulla privacy. Selezionare l'opzione **Accetto l'Informativa sulla privacy** solo se si accetta che i dati vengano gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy.
7. Selezionare un file (dall'elenco dei file estratti dal file di archivio scelto) e specificare i parametri della riga di comando di un file eseguibile.

   È possibile specificare i parametri della riga di comando per installare l'applicazione dal pacchetto di installazione in modalità automatica. Specificare i parametri della riga di comando è un'operazione facoltativa.

   Viene avviata la procedura per creare il pacchetto di installazione.

   La procedura guidata informa l'utente al termine della procedura.

   Se il pacchetto di installazione non viene creato, viene visualizzato un messaggio appropriato.
8. Fare clic sul pulsante **Fine** per chiudere la procedura guidata.

Il pacchetto di installazione creato viene scaricato nella sottocartella Pacchetti della cartella condivisa di Administration Server. Dopo il download, il pacchetto di installazione viene visualizzato nell'elenco dei pacchetti di installazione.

Nell'elenco dei pacchetti di installazione disponibili in Administration Server, facendo clic sul collegamento con il nome di un pacchetto di installazione personalizzato, è possibile:

- Visualizzare le seguenti proprietà di un pacchetto di installazione:
  - **Nome**. Nome del pacchetto di installazione personalizzato.
  - **Origine**. Nome del produttore dell'applicazione.
  - **Applicazione**. Nome dell'applicazione inclusa nel pacchetto di installazione personalizzato.
  - **Versione**. Versione applicazione.
  - **Lingua**. Lingua dell'applicazione inclusa nel pacchetto di installazione personalizzato.
  - **Dimensioni (MB)**. Dimensioni del pacchetto di installazione.
  - **Sistema operativo**. Tipo di sistema operativo a cui è destinato il pacchetto di installazione.
  - **Data creazione**. Data di creazione del pacchetto di installazione.
  - **Ultima modifica**. Data di modifica del pacchetto di installazione.
  - **Tipo**. Tipo di pacchetto di installazione.
- Modificare i parametri della riga di comando.

Creazione di pacchetti di installazione indipendenti

Gli utenti dei dispositivi nell'organizzazione possono utilizzare pacchetti di installazione indipendenti per installare manualmente le applicazioni nei dispositivi.

Un pacchetto di installazione indipendente è un file eseguibile che può essere archiviato nel server Web o nella cartella condivisa, inviato tramite e-mail o trasferito a un dispositivo client utilizzando un altro metodo. Nel dispositivo client l'utente può eseguire il file ricevuto in locale per installare un'applicazione senza coinvolgere Kaspersky Security Center Linux. È possibile creare pacchetti di installazione indipendenti per le applicazioni Kaspersky e per applicazioni di terzi. Per creare un pacchetto di installazione indipendente per un'applicazione di terzi, è necessario creare un pacchetto di installazione personalizzato.

Assicurarsi che il pacchetto di installazione indipendente non sia disponibile per terze persone.

Per creare un pacchetto di installazione indipendente:

1. Eseguire una delle seguenti operazioni:
   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.

- Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Nell'elenco dei pacchetti di installazione selezionare un pacchetto di installazione e, sopra l'elenco, fare clic sul pulsante **Distribuisci**.

3. Selezionare l'opzione **Utilizzo di un pacchetto indipendente**.

   Verrà avviata la Creazione guidata pacchetto di installazione indipendente. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Assicurarsi che l'opzione **Installa Network Agent con questa applicazione**, se si desidera installare Network Agent insieme all'applicazione selezionata.

   Per impostazione predefinita, questa opzione è abilitata. È consigliabile abilitare questa opzione se non si è sicuri che Network Agent sia installato nel dispositivo. Se Network Agent è già installato nel dispositivo, dopo l'installazione del pacchetto di installazione indipendente con Network Agent, Network Agent verrà aggiornato alla versione più recente.

   Se si disabilita questa opzione, Network Agent non verrà installato nel dispositivo e il dispositivo non sarà gestito.

   Se un pacchetto di installazione indipendente per l'applicazione selezionata esiste già in Administration Server, la procedura guidata informa l'utente. In questo caso, è necessario selezionare una delle seguenti azioni:

   - **Crea pacchetto di installazione indipendente**. Selezionare questa opzione se ad esempio si desidera creare un pacchetto di installazione indipendente per una nuova versione dell'applicazione e si desidera mantenere anche un pacchetto di installazione indipendente creato per una versione precedente dell'applicazione. Il nuovo pacchetto di installazione indipendente viene inserito in un'altra cartella.

   - **Usa pacchetto di installazione indipendente esistente**. Selezionare questa opzione se si desidera utilizzare un pacchetto di installazione indipendente esistente. Il processo di creazione del pacchetto non verrà avviato.

   - **Ricrea pacchetto di installazione indipendente esistente**. Selezionare questa opzione se si desidera creare nuovamente un pacchetto di installazione indipendente per la stessa applicazione. Il pacchetto di installazione indipendente viene inserito nella stessa cartella.

5. Nel passaggio **Sposta nell'elenco dei dispositivi gestiti**, l'opzione **Non spostare i dispositivi** è selezionata per impostazione predefinita. Se non si desidera spostare il dispositivo client in un gruppo di amministrazione dopo l'installazione di Network Agent, non modificare la scelta dell'opzione.

   Se si desidera spostare il dispositivo client dopo l'installazione di Network Agent, selezionare l'opzione **Sposta i dispositivi non assegnati in questo gruppo** e specificare un gruppo di amministrazione in cui spostare il dispositivo client. Per impostazione predefinita, il dispositivo viene spostato nel gruppo **Dispositivi gestiti**.

6. Al termine del processo di creazione del pacchetto di installazione indipendente, fare clic sul pulsante **FINE**.

   La Creazione guidata pacchetto di installazione indipendente verrà chiusa.

Il pacchetto di installazione indipendente viene creato e inserito nella sottocartella PkgInst della cartella condivisa di Administration Server. È possibile visualizzare l'elenco dei pacchetti indipendenti facendo clic sul pulsante **Visualizza l'elenco dei pacchetti indipendenti** sopra l'elenco dei pacchetti di installazione.

Modifica del limite relativo alle dimensioni dei dati del pacchetto di installazione personalizzato

Le dimensioni totali dei dati decompressi durante la creazione di un pacchetto di installazione personalizzato sono limitate. Il limite predefinito è 1 GB.

Se si tenta di caricare un file di archivio contenente dati che superano il limite corrente, viene visualizzato un messaggio di errore. Potrebbe essere necessario aumentare questo valore limite durante la creazione dei pacchetti di installazione a partire da pacchetti di distribuzione di grandi dimensioni.

Per modificare il valore limite per le dimensioni del pacchetto di installazione personalizzato:

1. Nel dispositivo Administration Server, eseguire il prompt dei comandi con l'account utilizzato per installare Administration Server.
2. Modificare la directory corrente nella cartella di installazione di Kaspersky Security Center Linux (in genere, /opt/kaspersky/ksc64/sbin).
3. A seconda del tipo di installazione del server di amministrazione, immettere uno dei seguenti comandi nell'account root:

   - Installazione locale normale:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <numero di byte>
     ```

   - Installazione nel cluster di failover Kaspersky Security Center Linux:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <numero di byte> --stp klfoc
     ```

   Dove <numero di byte> è un numero di byte in formato esadecimale o decimale.

   Ad esempio, se il limite richiesto è 2 GB, è possibile specificare il valore decimale 2147483648 o il valore esadecimale 0x80000000. In questo caso, per un'installazione locale di Administration Server, è possibile utilizzare il seguente comando:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Il limite relativo alle dimensioni dei dati del pacchetto di installazione personalizzato è stato modificato.

Installazione di Network Agent per Linux in modalità automatica (con un file di risposte)

È possibile installare Network Agent nei dispositivi Linux utilizzando un file di risposte, vale a dire un file di testo contenente un set personalizzato di parametri di installazione: variabili e rispettivi valori. L'uso di questo file di risposte consente di eseguire un'installazione in modalità automatica, ovvero senza la partecipazione dell'utente.

Per eseguire l'installazione di Network Agent per Linux in modalità automatica:

1. Se si desidera installare Network Agent nei dispositivi con sistema operativo SUSE Linux Enterprise Server 15, installare il pacchetto insserv-compat prima di configurare Network Agent.
2. Leggere il Contratto di licenza con l'utente finale. Seguire i passaggi di seguito solo se sono stati compresi e accettati i termini del Contratto di licenza con l'utente finale.
3. Impostare il valore della variabile di ambiente KLAUTOANSWERS nell'ambiente radice o utente inserendo il nome completo del file di risposte (incluso il percorso), ad esempio come segue:

   ```
   export KLAUTOANSWERS=/tmp/nagent_install/answers.txt
   ```

4. Creare il file di risposte (in formato TXT) nella directory specificata nella variabile di ambiente. Aggiungere al file di risposte un elenco di variabili nel formato NOME_VARIABILE=valore_variabile, ognuna su una riga separata.

   Per il corretto utilizzo del file di risposte, è necessario includere un set minimo delle tre variabili richieste:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   È inoltre possibile aggiungere eventuali variabili opzionali per utilizzare parametri più specifici dell'installazione remota. La tabella seguente elenca tutte le variabili che possono essere incluse nel file di risposte:

   Variabili del file di risposte utilizzate come parametri dell'installazione di Network Agent per Linux in modalità automatica

Variabili del file di risposte utilizzate come parametri dell'installazione di Network Agent per Linux in modalità automatica

Nome della variabile	Richiesto	Descrizione	Valori possibili
KLNAGENT_SERVER	Sì	Contiene il nome di Administration Server sotto forma di nome di dominio completo (FQDN) o indirizzo IP.	Nome DNS o indirizzo IP.
KLNAGENT_AUTOINSTALL	Sì	Indica se la modalità di installazione automatica è abilitata.	1—La modalità automatica è abilitata; l'utente non deve eseguire alcuna operazione durante l'installazione. Altro—La modalità automatica è disabilitata; all'utente può essere richiesto di eseguire operazioni durante l'installazione.
EULA_ACCEPTED	Sì	Indica se l'utente accetta il Contratto di licenza con l'utente finale (EULA) di Network Agent; se non disponibile, può essere interpretato come la mancata accettazione dell'EULA.	1 - Confermo di aver letto, compreso e accettato i termini e le condizioni del presente Contratto di licenza con l'utente finale Altro o non specificato—Non accetto i termini del Contratto di licenza (l'installazione non viene eseguita).
KLNAGENT_PROXY_USE	No	Indica se la connessione con Administration Server utilizzerà le impostazioni del proxy. Il valore predefinito è 0.	1—Le impostazioni del proxy vengono utilizzate. Altro—Le impostazioni del proxy non vengono utilizzate.
KLNAGENT_PROXY_ADDR	No	Indica l'indirizzo del server proxy utilizzato per la connessione con Administration Server.	Nome DNS o indirizzo IP.
KLNAGENT_PROXY_LOGIN	No	Indica il nome utente utilizzato per l'accesso al server proxy.	Qualsiasi nome utente esistente.
KLNAGENT_PROXY_PASSWORD	No	Indica la password utente utilizzata per l'accesso al server proxy.	Qualsiasi set di caratteri alfanumerici consentiti dal formato password nel sistema operativo.
KLNAGENT_VM_VDI	No	Indica se Network Agent è installato in un'immagine per la creazione di macchine virtuali dinamiche.	1—Network Agent è installato in un'immagine, che verrà successivamente utilizzata per la creazione di macchine virtuali dinamiche. Altro—Non viene utilizzata alcuna immagina durante l'installazione.
KLNAGENT_VM_OPTIMIZE	No	Indica se le impostazioni di Network Agent sono ottimali per l'hypervisor.	1—Le impostazioni locali predefinite di Network Agent vengono modificate per consentire l'utilizzo ottimizzato nell'hypervisor.
KLNAGENT_TAGS	No	Elenca i tag assegnati all'istanza di Network Agent.	Uno o più nomi di tag separati da un punto e virgola.
KLNAGENT_UDP_PORT	No	Indica la porta UDP utilizzata da Network Agent. Il valore predefinito è 15000.	Qualsiasi numero di porta esistente.
KLNAGENT_PORT	No	Definisce la porta non TLS utilizzata da Network Agent. Il valore predefinito è 14000.	Qualsiasi numero di porta esistente.
KLNAGENT_SSLPORT	No	Definisce la porta TLS utilizzata da Network Agent. Il valore predefinito è 13000.	Qualsiasi numero di porta esistente.
KLNAGENT_USESSL	No	Indica se per la connessione viene utilizzato Transport Layer Security (TLS).	1 (predefinito)—TLS viene utilizzato. Altro—TLS non viene utilizzato.
KLNAGENT_GW_MODE	No	Indica se viene utilizzato il gateway di connessione.	1 (predefinito)—Le impostazioni correnti non vengono modificate (alla prima chiamata non viene specificato alcun gateway di connessione).

			2—Non viene utilizzato alcun gateway di connessione. 3—Il gateway di connessione viene utilizzato. KLNAGENT_GW_ADDRESS è obbligatorio. 4—L'istanza di Network Agent viene utilizzata come gateway di connessione nella rete perimetrale (DMZ). Il certificato del server è obbligatorio.
KLNAGENT_GW_ADDRESS	No	Indica l'indirizzo del gateway di connessione. Il valore è applicabile solo se KLNAGENT_GW_MODE=3.	Nome DNS o indirizzo IP.

5. Installazione di Network Agent:

   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 32 bit, eseguire il comando seguente:
     `# yum install ./klnagent-<numero build>.i386.rpm`
   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 64 bit, eseguire il comando seguente:
     `# yum install ./klnagent64-<numero build>.x86_64.rpm`
   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 64 bit per l'architettura Arm, eseguire il comando seguente:
     `# yum install ./klnagent64-<numero build>.aarch64.rpm`
   - Per installare Network Agent da un pacchetto DEB in un sistema operativo a 32 bit, eseguire il comando seguente:
     `# apt-get install ./klnagent_<numero build>_i386.deb`
   - Per installare Network Agent da un pacchetto DEB in un sistema operativo a 64 bit, eseguire il comando seguente:
     `# apt-get install ./klnagent64_<numero build>_amd64.deb`
   - Per installare Network Agent da un pacchetto DEB in un sistema operativo a 64 bit per l'architettura Arm, eseguire il comando seguente:
     `# apt-get install ./klnagent64_<numero build>_arm64.deb`

   Per installare Network Agent nell'ambiente utente, aggiungere `sudo -E` prima del comando. Ad esempio, per installare Network Agent da un pacchetto RPM su un sistema operativo a 32 bit, eseguire il seguente comando:

   `$ sudo -E yum install ./klnagent-<numero build>.i386.rpm`

   L'installazione di Network Agent per Linux viene avviata in modalità automatica; all'utente non viene richiesto di eseguire alcuna operazione durante il processo.

Preparazione di un dispositivo in cui viene eseguito Astra Linux in modalità ambiente software chiuso per l'installazione di Network Agent

Prima di installare Network Agent in un dispositivo in cui viene esegue Astrito Linux in modalità ambiente software chiuso, è necessario eseguire due procedure di preparazione: quella nelle istruzioni riportate di seguito e i passaggi generali di preparazione per qualsiasi dispositivo Linux.

Prima di iniziare:

- Verificare che il dispositivo in cui si desidera installare Network Agent for Linux esegua una delle distribuzioni Linux supportate.
- Scaricare il file di installazione di Network Agent necessario dal sito Web di Kaspersky.

Eseguire i comandi presenti in questa istruzione con un account con privilegi di root.

Per preparare un dispositivo in cui viene eseguito Astra Linux in modalità ambiente software chiuso per l'installazione di Network Agent:

1. Aprire il file `/etc/digsig/digsig_initramfs.conf`, quindi specificare la seguente impostazione:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Nella riga di comando, eseguire il seguente comando per installare il pacchetto di compatibilità:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Creare una directory per la chiave dell'applicazione:

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

4. Posizionare la chiave dell'applicazione /opt/kaspersky/ksc64/share/kaspersky_astra_pub_key.gpg nella directory creata nel passaggio precedente:

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

   Se il kit di distribuzione di Kaspersky Security Center Linux non include la chiave dell'applicazione kaspersky_astra_pub_key.gpg, è possibile scaricarla facendo clic sul collegamento: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Aggiornare i dischi RAM:

   ```
   update-initramfs -u -k all
   ```

   Riavviare il sistema.

6. Eseguire i passaggi di preparazione comuni per qualsiasi dispositivo Linux.

Il dispositivo è preparato. È ora possibile procedere all'installazione di Network Agent.

Visualizzazione dell'elenco dei pacchetti di installazione indipendenti

È possibile visualizzare l'elenco dei pacchetti di installazione indipendenti e le proprietà di ciascun pacchetto di installazione indipendente.

Per visualizzare l'elenco dei pacchetti di installazione indipendenti per tutti i pacchetti di installazione:

Sopra l'elenco, fare clic sul pulsante **Visualizza l'elenco dei pacchetti indipendenti**.

Nell'elenco dei pacchetti di installazione indipendenti le relative proprietà vengono visualizzate come segue:

- **Nome pacchetto**. Nome del pacchetto di installazione indipendente, formato automaticamente dal nome dell'applicazione incluso nel pacchetto e dalla versione dell'applicazione.
- **Nome applicazione**. Nome dell'applicazione incluso nel pacchetto di installazione indipendente.
- **Versione applicazione**.
- **Nome pacchetto di installazione di Network Agent**. La proprietà viene visualizzata solo se Network Agent è incluso nel pacchetto di installazione indipendente.
- **Versione di Network Agent**. La proprietà viene visualizzata solo se Network Agent è incluso nel pacchetto di installazione indipendente.
- **Dimensione**. Dimensione del file in MB.
- **Gruppo**. Nome del gruppo in cui viene spostato il dispositivo client dopo l'installazione di Network Agent.
- **Data creazione**. Data e ora di creazione del pacchetto di installazione indipendente.
- **Ultima modifica**. Data e ora di modifica del pacchetto di installazione indipendente.
- **Percorso**. Percorso completo della cartella in cui si trova il pacchetto di installazione indipendente.
- **Indirizzo Web**. Indirizzo Web del pacchetto di installazione indipendente.
- **Hash del file**. La proprietà viene utilizzata per certificare che il pacchetto di installazione indipendente non è stato modificato da terze parti e che un utente ha lo stesso file che è stato creato e trasferito all'utente.

Per visualizzare l'elenco dei pacchetti di installazione indipendenti per un pacchetto di installazione specifico:

Selezionare il pacchetto di installazione nell'elenco e, sopra l'elenco, fare clic sul pulsante **Visualizza l'elenco dei pacchetti indipendenti**.

Nell'elenco dei pacchetti di installazione indipendenti è possibile eseguire le seguenti operazioni:

- Pubblicare un pacchetto di installazione indipendente sul server Web facendo clic sul pulsante **Pubblica**. Il pacchetto di installazione indipendente pubblicato è disponibile per il download per gli utenti a cui è stato inviato il collegamento al pacchetto di installazione indipendente.
- Annullare la pubblicazione di un pacchetto di installazione indipendente sul server Web facendo clic sul pulsante **Annulla pubblicazione**. Il pacchetto di installazione indipendente non pubblicato è disponibile per il download solo per gli amministratori.
- Scaricare un pacchetto di installazione indipendente nel dispositivo facendo clic sul pulsante **Scarica**.
- Inviare un messaggio e-mail con il collegamento a un pacchetto di installazione indipendente facendo clic sul pulsante **Invia tramite e-mail**.
- Rimuovere un pacchetto di installazione indipendente facendo clic sul pulsante **Rimuovi**.

Distribuzione dei pacchetti di installazione agli Administration Server secondari

Kaspersky Security Center Linux consente di creare pacchetti di installazione per le applicazioni Kaspersky e per le applicazioni di terzi, nonché distribuire i pacchetti di installazione ai dispositivi client e installare le applicazioni dai pacchetti. Per ottimizzare il carico sull'Administration Server primario, è possibile distribuire i pacchetti di installazione agli Administration Server secondari. Successivamente, i server secondari trasmettono i pacchetti ai dispositivi client e quindi è possibile eseguire l'installazione remota delle applicazioni nei dispositivi client.

Per distribuire i pacchetti di installazione agli Administration Server secondari:

1. Assicurarsi che tutti gli Administration Server secondari siano connessi all'Administration Server primario.
2. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

   Verrà visualizzato l'elenco delle attività.
3. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
4. Nella pagina **Nuova attività**, nell'elenco a discesa **Applicazione** selezionare **Kaspersky Security Center**. Quindi, nell'elenco a discesa **Tipo di attività**, selezionare **Distribuisci pacchetto di installazione** e specificare il nome dell'attività.
5. Nella pagina **Ambito attività**, selezionare i dispositivi a cui è assegnata l'attività in uno dei seguenti modi:

   - Se si desidera creare un'attività per tutti gli Administration Server secondari in un gruppo di amministrazione specifico, selezionare questo gruppo e quindi creare un'attività di gruppo per questo.
   - Se si desidera creare un'attività per Administration Server secondari specifici, selezionare questi server e quindi creare un'attività per questi.
6. Nella pagina **Pacchetti di installazione da distribuire**, selezionare i pacchetti di installazione da copiare negli Administration Server secondari.
7. Specificare un account per eseguire l'attività *Distribuisci pacchetto di installazione* in questo account. È possibile utilizzare il proprio account e mantenere abilitata l'opzione **Account predefinito**. In alternativa, è possibile specificare che l'attività deve essere eseguita con un altro account che disponga dei diritti di accesso necessari. A tale scopo, selezionare l'opzione **Specifica account**, quindi immettere le credenziali di tale account.
8. Nella pagina **Completa creazione attività**, è possibile abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** per aprire la finestra delle proprietà dell'attività, quindi modificare le impostazioni predefinite dell'attività. In caso contrario, è possibile configurare le impostazioni dell'attività in un secondo momento, quando desiderato.
9. Fare clic sul pulsante **Fine**.

   L'attività creata per la distribuzione dei pacchetti di installazione agli Administration Server secondari viene visualizzata nell'elenco delle attività.
10. È possibile eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività, i pacchetti di installazione selezionati vengono copiati negli Administration Server secondari specificati.

Preparazione di un dispositivo Linux e installazione di Network Agent in un dispositivo Linux da remoto

L'installazione di Network Agent comprende due passaggi:

- Una preparazione per il dispositivo Linux
- Installazione remota di Network Agent

Una preparazione per il dispositivo Linux

Per preparare un dispositivo Linux per l'installazione remota di Network Agent:

1. Accertarsi che il seguente software sia installato nel dispositivo Linux di destinazione.
   - Sudo (per Ubuntu 10.04, la versione di Sudo è 1.7.2p1 o successiva)
   - Interprete del linguaggio Perl versione 5.10 o successiva
2. Testare la configurazione del dispositivo:
   a. Verificare se è possibile connettersi al dispositivo tramite un client SSH (ad esempio, PuTTY).

      Se non è possibile connettersi al dispositivo, aprire il file `/etc/ssh/sshd_config` e verificare che per le seguenti impostazioni siano specificati i valori elencati:

      ```
      PasswordAuthentication no
      ChallengeResponseAuthentication yes
      ```

      > Non modificare il file /etc/ssh/sshd_config se è possibile connettersi al dispositivo senza problemi; in caso contrario, è possibile che si verifichi un errore di autenticazione SSH durante l'esecuzione di un'attività di installazione remota.

      Salvare il file (se necessario) e riavviare il servizio SSH utilizzando il comando `sudo service ssh restart`.

   b. Disabilitare la password sudo per l'account utente con cui deve essere eseguita la connessione del dispositivo.

   c. Utilizzare il comando `visudo` in sudo per aprire il file di configurazione sudoers.

      Nel file aperto, aggiungere la seguente riga alla fine del file: `<nome utente> ALL = (ALL) NOPASSWD: ALL`. In questo caso, `<username>` è l'account utente che deve essere utilizzato per la connessione del dispositivo tramite SSH. Se si utilizza il sistema operativo Astra Linux, nel file /etc/sudoers aggiungere l'ultima riga con il seguente testo: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Salvare e chiudere il file sudoers.

   e. Eseguire di nuovo la connessione al dispositivo tramite SSH e verificare che il servizio Sudo non richieda l'immissione di una password. A tale scopo, utilizzare il comando `sudo whoami`.

3. Aprire il file `/etc/systemd/logind.conf`, quindi eseguire una delle seguenti operazioni:
   - Specificare "no" come valore per l'impostazione KillUserProcesses: `KillUserProcesses=no`.
   - Per l'impostazione KillExcludeUsers digitare il nome utente dell'account con il quale deve essere eseguita l'installazione remota, ad esempio, `KillExcludeUsers=root`.

Se nel dispositivo di destinazione viene eseguito Astra Linux, aggiungere la stringa `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` nel file `/home/<nome utente>/.bashrc`, dove `<nome utente>` è l'account utente da utilizzare per la connessione del dispositivo tramite SSH.

Per applicare l'impostazione modificata, riavviare il dispositivo Linux o eseguire il seguente comando:

```
$ sudo systemctl restart systemd-logind.service
```

4. Se si desidera installare Network Agent nei dispositivi con sistema operativo SUSE Linux Enterprise Server 15, installare il pacchetto insserv-compat prima di configurare Network Agent.

5. Se si desidera installare Network Agent nei dispositivi con il sistema operativo Astra Linux in esecuzione in modalità ambiente software chiuso, eseguire passaggi aggiuntivi per preparare i dispositivi Astra Linux.

6. Se si desidera installare Network Agent nei dispositivi con il sistema operativo RED OS 7.3.4 o versione successiva o MSVSPHERE 9.2 o versione successiva, installare il pacchetto libxcrypt-compat per il corretto funzionamento di Network Agent.

Installazione remota di Network Agent

Per installare Network Agent nei dispositivi Linux da remoto:

1. Scaricare e creare un pacchetto di installazione:

   a. Prima di installare il pacchetto nel dispositivo, verificare di avere già installato tutte le dipendenze (programmi e librerie) per questo pacchetto.

   È possibile visualizzare le dipendenze per ciascun pacchetto autonomamente, utilizzando le utilità specifiche per la distribuzione Linux in cui deve essere installato il pacchetto. Per informazioni dettagliate sulle utilità, fare riferimento alla documentazione del sistema operativo.

   b. Scaricare il pacchetto di installazione di Network Agent utilizzando l'interfaccia dell'applicazione o dal sito Web di Kaspersky.

   c. Per creare un pacchetto di installazione remota, utilizzare i seguenti file:

   - klnagent.kpd
   - akinstall.sh
   - Pacchetto .deb o .rpm di Network Agent

2. Crea un'attività di installazione remota con le seguenti impostazioni:

   - Nella pagina **Impostazioni** della Creazione guidata nuova attività, selezionare la casella di controllo **Utilizzo delle risorse del sistema operativo tramite Administration Server**. Deselezionare tutte le altre caselle di controllo.
   - Nella pagina **Selezione di un account per l'esecuzione dell'attività**, specificare le impostazioni dell'account utente utilizzato per la connessione del dispositivo tramite SSH.

3. Eseguire l'attività di installazione remota. Utilizzare l'opzione per il comando `su` per preservare l'ambiente: `-m, -p, --preserve-environment`.

Installazione delle applicazioni tramite un'attività di installazione remota

Kaspersky Security Center Linux consente di installare le applicazioni nei dispositivi in remoto, utilizzando le attività di installazione remota. Tali attività vengono create e assegnate ai dispositivi attraverso un'apposita procedura guidata. Per assegnare un'attività più in modo facile e rapido, è possibile specificare i dispositivi (fino a 1000 dispositivi) nella finestra della procedura guidata in uno dei seguenti modi:

- **Assegna un'attività a un gruppo di amministrazione**. In questo caso l'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione creato precedentemente.
- **Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco**. È possibile specificare nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.
- **Assegna un'attività a una selezione dispositivi**. In questo caso l'attività viene assegnata ai dispositivi inclusi in una selezione creata precedentemente. È possibile specificare la selezione predefinita o una selezione personalizzata creata. È possibile selezionare solo fino a 1000 dispositivi.

Per evitare problemi che possono verificarsi durante l'installazione dell'applicazione in un dispositivo client senza Network Agent installato, è necessario procedere come descritto nella distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center Linux.

Installazione remota di un'applicazione

Questa sezione contiene informazioni su come installare un'applicazione nei dispositivi in remoto in un gruppo di amministrazione, in dispositivi con indirizzi IP specifici o in una selezione di dispositivi.

Per installare un'applicazione in dispositivi specifici:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.
3. Nel campo **Tipo di attività**, selezionare **Installa l'applicazione in remoto**.
4. Selezionare una delle seguenti opzioni:

   - Assegna attività a un gruppo di amministrazione

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

     Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

   - Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco

È possibile specificare nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

- **Assegna attività a una selezione dispositivi**

  L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

Viene creata l'attività *Installa l'applicazione in remoto* per i dispositivi specificati. Se è stata selezionata l'opzione **Assegna attività a un gruppo di amministrazione**, si tratta di un'attività di gruppo.

5. Nel passaggio **Ambito attività**, specificare un gruppo di amministrazione, dispositivi con indirizzi IP specifici o una selezione di dispositivi.

   Le impostazioni disponibili dipendono dall'opzione selezionata nel passaggio precedente.

6. Nel passaggio **Pacchetti di installazione**, specificare le seguenti impostazioni:

   - Nel campo **Selezionare il pacchetto di installazione**, selezionare il pacchetto di installazione di un'applicazione da installare.

   - Nel gruppo di impostazioni **Forza il download del pacchetto di installazione** specificare la modalità di distribuzione dei file necessari per l'installazione dell'applicazione ai dispositivi client:

     - **Utilizzando Network Agent**

       Se questa opzione è abilitata, i pacchetti di installazione vengono distribuiti ai dispositivi client da Network Agent installato nei dispositivi client.

       Se questa opzione è disabilitata, i pacchetti di installazione vengono distribuiti utilizzando gli strumenti del sistema operativo dei dispositivi client.

       È consigliabile abilitare questa opzione se l'attività è stata assegnata a dispositivi in cui sono installati Network Agent.

       Per impostazione predefinita, questa opzione è abilitata.

     - **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**

Se questa opzione è abilitata, i pacchetti di installazione verranno trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo tramite i punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete.

Se l'opzione **Utilizzo di Network Agent** è abilitata, i file vengono inviati tramite gli strumenti del sistema operativo solo se gli strumenti di Network Agent non sono disponibili.

Per impostazione predefinita, questa opzione è abilitata per le attività di installazione remota create in un Administration Server virtuale.

L'unico modo per installare un'applicazione per Windows (incluso Network Agent per Windows) in un dispositivo in cui non è installato Network Agent consiste nell'utilizzare un punto di distribuzione basato su Windows. Pertanto, quando si installa un'applicazione Windows:

- Selezionare questa opzione.
- Assicurarsi che sia assegnato un punto di distribuzione per i dispositivi client di destinazione.
- Assicurarsi che il punto di distribuzione sia basato su Windows.

- **Utilizzando le risorse del sistema operativo tramite Administration Server**

  Se questa opzione è selezionata, i file vengono trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo dei dispositivi client tramite l'Administration Server. È possibile abilitare questa opzione se Network Agent non è installato nel dispositivo client, ma il dispositivo client si trova nella stessa rete di Administration Server.

  Per impostazione predefinita, questa opzione è abilitata.

- Nel campo **Numero massimo di download simultanei**, specificare il numero massimo consentito di dispositivi client a cui Administration Server può trasmettere simultaneamente i file.

- Nel campo **Numero massimo di tentativi di installazione**, specificare il numero massimo consentito di esecuzioni del programma di installazione.

  Se il numero di tentativi specificato nel parametro viene superato, Kaspersky Security Center Linux non avvia più il programma di installazione nel dispositivo. Per riavviare l'attività *Installa l'applicazione in remoto*, aumentare il valore del parametro **Numero massimo di tentativi di installazione** e avviare l'attività. In alternativa, è possibile creare una nuova attività *Installa l'applicazione in remoto*.

- Definire l'impostazione aggiuntiva:

  - **Non reinstallare l'applicazione se è già installata**

    Se questa opzione è abilitata, l'applicazione selezionata non verrà reinstallata se è già stata installata nel dispositivo client.

    Se questa opzione è disabilitata, l'applicazione verrà installata in ogni caso.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Verifica il tipo di sistema operativo prima del download**

Prima di trasmettere i file ai dispositivi client, Kaspersky Security Center Linux verifica se le impostazioni dell'utilità di installazione sono applicabili al sistema operativo del dispositivo client. Se le impostazioni non sono applicabili, Kaspersky Security Center Linux non trasmette i file e non tenta di installare l'applicazione. Ad esempio, per installare un'applicazione nei dispositivi di un gruppo di amministrazione che include dispositivi che eseguono vari sistemi operativi, è possibile assegnare l'attività di installazione al gruppo di amministrazione e quindi abilitare questa opzione per ignorare i dispositivi che eseguono un sistema operativo diverso da quello desiderato.

- **Chiedi agli utenti di chiudere le applicazioni in esecuzione**

  L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

  Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

  Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

  Per impostazione predefinita, questa opzione è disabilitata.

- Selezionare in quali dispositivi installare l'applicazione:

  - **Installa in tutti i dispositivi**

    L'applicazione verrà installata anche nei dispositivi gestiti da altri Administration Server.

    Questa opzione è selezionata per impostazione predefinita. Non è necessario modificare l'impostazione se si dispone di un solo Administration Server nella rete.

  - **Installa solo nei dispositivi gestiti tramite questo Administration Server**

    L'applicazione verrà installata solo nei dispositivi gestiti da questo Administration Server. Selezionare questa opzione se si dispone di più Administration Server nella rete per evitare conflitti tra di essi.

- Specificare se i dispositivi devono essere spostati in un gruppo di amministrazione dopo l'installazione:

  - **Non spostare i dispositivi**

    I dispositivi rimangono nei gruppi in cui si trovano attualmente. I dispositivi che non sono stati inseriti in alcun gruppo rimangono non assegnati.

  - **Sposta i dispositivi non assegnati nel gruppo selezionato (è possibile selezionare un solo gruppo)**

    I dispositivi vengono spostati nel gruppo di amministrazione selezionato.

  Nota: l'opzione **Non spostare i dispositivi** è selezionata per impostazione predefinita. Per motivi di sicurezza, è consigliabile spostare i dispositivi manualmente.

7. In questo passaggio della procedura guidata, specificare se i dispositivi devono essere riavviati durante l'installazione delle applicazioni:

- **Non riavviare il dispositivo**

  Se questa opzione è selezionata, il dispositivo non verrà riavviato dopo l'installazione dell'applicazione di protezione.

- **Riavvia il dispositivo**

  Se questa opzione è selezionata, il dispositivo verrà riavviato dopo l'installazione dell'applicazione di protezione.

8. Se necessario, nel passaggio **Selezionare gli account per l'accesso ai dispositivi** è possibile aggiungere gli account che verranno utilizzati per avviare l'attività *Installa l'applicazione in remoto*:

   - **Nessun account richiesto (Network Agent installato)**

     Se questa opzione è selezionata, non è necessario specificare un account con cui verrà eseguito il programma di installazione dell'applicazione. L'attività sarà eseguita tramite l'account con cui viene eseguito Administration Server.

     Se Network Agent non è stato installato nei dispositivi client, questa opzione non è disponibile.

   - **Account richiesto (Network Agent non utilizzato)**

     Selezionare questa opzione se Network Agent non è installato nei dispositivi a cui si assegna l'attività di installazione remota. In questo caso, è possibile specificare un account utente o un certificato SSH per installare l'applicazione.

     - **Account locale**. Se questa opzione è selezionata, specificare l'account utente con cui verrà eseguito il programma di installazione dell'applicazione. Fare clic sul pulsante **Aggiungi**, selezionare **Account locale** e quindi specificare le credenziali dell'account utente.

       È possibile specificare più account utente, ad esempio se nessuno di essi dispone di tutti i diritti richiesti per tutti i dispositivi per cui si assegna l'attività. In questo caso, tutti gli account aggiunti vengono utilizzati per l'esecuzione dell'attività, consecutivamente, dall'alto in basso.

     - **Certificato SSH**. Se si desidera installare un'applicazione in un dispositivo client basato su Linux, è possibile specificare un certificato SSH anziché un account utente. Fare clic sul pulsante **Aggiungi**, selezionare **Certificato SSH**, quindi specificare la chiave privata e quella pubblica del certificato.

       Per generare una chiave privata, è possibile utilizzare l'utilità ssh-keygen. Kaspersky Security Center Linux supporta il formato PEM delle chiavi private, ma l'utilità ssh-keygen genera chiavi SSH nel formato OPENSSH per impostazione predefinita. Il formato OPENSSH non è supportato da Kaspersky Security Center Linux. Per creare una chiave privata nel formato PEM supportato, aggiungere l'opzione -m PEM nel comando ssh-keygen. Ad esempio:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail dell'utente>"
       ```

9. Nel passaggio **Completa creazione attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

   Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata la finestra delle impostazioni dell'attività. In questa finestra, è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio delle attività, se necessario.

10. Nell'elenco delle attività, selezionare l'attività creata, quindi fare clic su **Avvia**.

    In alternativa, attendere l'avvio dell'attività in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di installazione remota, l'applicazione selezionata viene installata nei dispositivi specificati.

Installazione di applicazioni negli Administration Server secondari

Per installare un'applicazione negli Administration Server secondari:

1. Stabilire una connessione all'Administration Server che controlla gli Administration Server secondari desiderati.
2. Verificare che il pacchetto di installazione corrispondente all'applicazione da installare sia disponibile in ognuno degli Administration Server secondari selezionati. Se non è possibile trovare il pacchetto di installazione in nessuno dei server secondari, è necessario distribuirlo. A tale scopo, creare un'attività con il tipo di attività **Distribuisci pacchetto di installazione**.
3. Creare un'attività per l'installazione remota di un'applicazione negli Administration Server secondari. Selezionare il tipo di attività **Installa l'applicazione nell'Administration Server secondario in remoto**.

   La Creazione guidata nuova attività crea un'attività per l'installazione remota dell'applicazione selezionata nella procedura guidata in determinati Administration Server secondari.
4. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di installazione remota, l'applicazione selezionata viene installata negli Administration Server secondari.

Definizione delle impostazioni per l'installazione remota nei dispositivi Unix

Quando si installa un'applicazione in un dispositivo Unix utilizzando un'attività di installazione remota, è possibile specificare le impostazioni specifiche per Unix per l'attività. Queste impostazioni sono disponibili nelle proprietà dell'attività dopo la creazione dell'attività.

Per specificare le impostazioni specifiche per Unix per un'attività di installazione remota:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul nome dell'attività di installazione remota per la quale si desidera specificare le impostazioni specifiche per Unix.

   Verrà visualizzata la finestra delle proprietà dell'attività.
3. Accedere a **Impostazioni applicazione** → **Impostazioni specifiche per Unix**.
4. Specificare le seguenti impostazioni:

   - **Imposta una password per l'account radice (solo per la distribuzione tramite SSH)**

Se il comando `sudo` non può essere utilizzato nel dispositivo di destinazione senza specificare la password, selezionare questa opzione, quindi specificare la password per l'account radice. Kaspersky Security Center Linux trasmette la password in formato criptato al dispositivo di destinazione, decripta la password e avvia la procedura di installazione per conto dell'account radice con la password specificata.

Kaspersky Security Center Linux non utilizza l'account o la password specificata per creare una connessione SSH.

- **Specifica il percorso di una cartella temporanea con autorizzazioni Esecuzione nel dispositivo di destinazione (solo per la distribuzione tramite SSH)**

  Se la directory /tmp nel dispositivo di destinazione non dispone dell'autorizzazione di esecuzione, selezionare questa opzione e specificare il percorso della directory con l'autorizzazione di esecuzione. Kaspersky Security Center Linux utilizza la directory specificata come directory temporanea per accedere tramite SSH. L'applicazione inserisce il pacchetto di installazione nella directory ed esegue la procedura di installazione.

5. Fare clic sul pulsante **Salva**.

Le impostazioni dell'attività specificata vengono salvate.

Avvio e arresto delle applicazioni Kaspersky.

È possibile utilizzare l'attività *Avvia o arresta l'applicazione* per avviare e arrestare le applicazioni Kaspersky nei dispositivi gestiti.

Per creare l'attività Avvia o arresta l'applicazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Nell'elenco a discesa **Applicazione**, selezionare l'applicazione per la quale si desidera creare l'attività.

   Le applicazioni Kaspersky vengono visualizzate nell'elenco se in precedenza sono stati aggiunti plug-in Web di gestione per tali applicazioni.
4. Nell'elenco **Tipo di attività**, selezionare l'attività **Attivazione dell'applicazione**.
5. Nel campo **Nome attività**, specificare il nome della nuova attività.

   Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
6. Selezionare i dispositivi a cui verrà assegnata l'attività.
7. Nella finestra **Applicazioni**, procedere come segue:

- Selezionare le caselle di controllo accanto ai nomi delle applicazioni per cui si desidera creare l'attività.
- Selezionare l'opzione **Avvia applicazione** o **Arresta applicazione**.

8. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nel passaggio **Completa creazione attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
9. Fare clic sul pulsante **Fine**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
10. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.
11. Nella finestra delle proprietà dell'attività, specificare le impostazioni generali dell'attività in base alle proprie esigenze, quindi salvare le impostazioni.

L'attività verrà creata e configurata.

Se si desidera eseguire l'attività, selezionarla nell'elenco delle attività, quindi fare clic sul pulsante **Avvia**.

Sostituzione di applicazioni di protezione di terzi

L'Installazione delle applicazioni di protezione Kaspersky tramite Kaspersky Security Center Linux può richiedere la rimozione di software di terzi incompatibile con l'applicazione da installare. Kaspersky Security Center Linux offre diversi modi di rimuovere le applicazioni di terzi.

Rimozione delle applicazioni incompatibili durante la configurazione dell'installazione remota di un'applicazione

È possibile abilitare l'opzione **Disinstalla automaticamente le applicazioni incompatibili** quando si configura l'installazione remota di un'applicazione di protezione nella Distribuzione guidata della protezione. Quando questa opzione è abilitata, Kaspersky Security Center Linux consente di rimuovere le applicazioni incompatibili prima di installare un'applicazione di protezione in un dispositivo gestito.

Rimozione delle applicazioni incompatibili tramite un'attività dedicata

Per rimuovere le applicazioni incompatibili, utilizzare l'attività *Disinstalla l'applicazione in remoto*. Questa attività deve essere eseguita nei dispositivi prima dell'attività di installazione dell'applicazione di protezione. Ad esempio, nell'attività di installazione è possibile selezionare il tipo di pianificazione **Al completamento di un'altra attività**, dove l'altra attività è *Disinstalla l'applicazione in remoto*.

Questo metodo di disinstallazione è consigliabile quando il programma di installazione dell'applicazione di protezione non è in grado di rimuovere correttamente un'applicazione incompatibile.

Rimozione di applicazioni o aggiornamenti software in remoto

È possibile rimuovere applicazioni o aggiornamenti software nei dispositivi gestiti in cui viene eseguito Linux da remoto solo tramite Network Agent.

Per rimuovere applicazioni o aggiornamenti software in remoto dai dispositivi selezionati:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Nell'elenco a discesa **Applicazione**, selezionare Kaspersky Security Center.
4. Nell'elenco **Tipo di attività**, selezionare il tipo di attività **Disinstalla l'applicazione in remoto**.
5. Nel campo **Nome attività**, specificare il nome della nuova attività.

   Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
6. Selezionare i dispositivi a cui verrà assegnata l'attività.

   Procedere al passaggio successivo della procedura guidata.
7. Selezionare il tipo di software da rimuovere, quindi selezionare specifiche applicazioni, aggiornamenti o patch che si desidera rimuovere:

   - **Disinstalla l'applicazione gestita**

     Verrà visualizzato un elenco di applicazioni Kaspersky. Selezionare l'applicazione che si desidera rimuovere.

   - **Disinstalla l'applicazione dal registro delle applicazioni**

Per impostazione predefinita, i Network Agent inviano ad Administration Server le informazioni sulle applicazioni installate nei dispositivi gestiti. L'elenco delle applicazioni installate è memorizzato nel Registro delle applicazioni.

Per selezionare un'applicazione dal Registro delle applicazioni:

a. Fare clic sul campo **Applicazione da disinstallare**, quindi selezionare l'applicazione che si desidera rimuovere.

Se si seleziona Kaspersky Security Center Network Agent, quando si esegue l'attività, lo stato *Completato correttamente* mostra che il processo di rimozione è stato avviato. Se Kaspersky Security Center Network Agent viene rimosso, lo stato non cambia. Se l'attività non riesce, lo stato diventa *Non riuscito*.

b. Specificare le opzioni di disinstallazione:

- Modalità di disinstallazione

Selezionare come si desidera rimuovere l'applicazione:

- **Definisci automaticamente il comando di disinstallazione**

  Se l'applicazione dispone di un comando di disinstallazione definito dal fornitore dell'applicazione, Kaspersky Security Center Linux utilizza questo comando. È consigliabile selezionare questa opzione.

- **Specificare il comando di disinstallazione**

  Selezionare questa opzione se si desidera specificare il proprio comando per la disinstallazione dell'applicazione.

  È consigliabile provare prima a rimuovere l'applicazione utilizzando l'opzione **Definisci automaticamente il comando di disinstallazione**. Se la disinstallazione tramite il comando definito automaticamente non va a buon fine, utilizzare il proprio comando.

  Digitare un comando di installazione nel campo, quindi specificare la seguente opzione:

  Usa questo comando per la disinstallazione solo se il comando predefinito non è stato rilevato automaticamente

  Kaspersky Security Center Linux controlla se l'applicazione selezionata dispone o meno di un comando di disinstallazione definito dal fornitore dell'applicazione. Se il comando viene rilevato, Kaspersky Security Center Linux lo utilizzerà al posto del comando specificato nel campo **Comando per la disinstallazione dell'applicazione**.

  È consigliabile abilitare questa opzione.

- Esegui il riavvio dopo la disinstallazione dell'applicazione

Se l'applicazione richiede il riavvio del sistema operativo nel dispositivo gestito dopo la disinstallazione, il sistema operativo viene riavviato automaticamente.

- Disinstalla l'aggiornamento dell'applicazione specificato, la patch o l'applicazione di terze parti specificata

Viene visualizzato un elenco di aggiornamenti, patch e applicazioni di terze parti. Selezionare l'elemento da rimuovere.

L'elenco visualizzato è un elenco generale di applicazioni e aggiornamenti e non corrisponde alle applicazioni e agli aggiornamenti installati nei dispositivi gestiti. Prima di selezionare un elemento, è consigliabile assicurarsi che l'applicazione o l'aggiornamento sia installato nei dispositivi definiti nell'ambito dell'attività. È possibile visualizzare l'elenco dei dispositivi in cui è installato l'aggiornamento o l'applicazione tramite la finestra delle proprietà.

Per visualizzare l'elenco dei dispositivi:

a. Fare clic sul nome dell'applicazione o dell'aggiornamento.

Verrà visualizzata la finestra delle proprietà.

b. Aprire la sezione **Dispositivi**.

È inoltre possibile visualizzare l'elenco delle applicazioni installate e degli aggiornamenti nella finestra delle proprietà del dispositivo.

8. Specificare il modo in cui i dispositivi client scaricheranno l'utilità di disinstallazione:

- **Utilizzando Network Agent**

  I file vengono distribuiti nei dispositivi client da Network Agent installato in tali dispositivi client.

  Se questa opzione è disabilitata, i file vengono distribuiti utilizzando gli strumenti del sistema operativo Linux.

  È consigliabile abilitare questa opzione se l'attività è stata assegnata a dispositivi in cui sono installati Network Agent.

- **Utilizzando le risorse del sistema operativo tramite Administration Server**

  L'opzione è obsoleta. Utilizzare l'opzione **Utilizzando Network Agent** o **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**.

  I file vengono trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo di Administration Server. È possibile abilitare questa opzione se Network Agent non è installato nel dispositivo client, ma il dispositivo client è incluso nella stessa rete di Administration Server.

- **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**

  I file vengono trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo tramite punti di distribuzione. È possibile abilitare questa opzione se è presente almeno un punto di distribuzione nella rete.

  Se l'opzione **Utilizzando Network Agent** è abilitata, i file vengono distribuiti utilizzando gli strumenti del sistema operativo solo se gli strumenti di Network Agent non sono disponibili.

- **Numero massimo di download simultanei**

Il numero massimo consentito di dispositivi client a cui Administration Server può trasmettere simultaneamente i file. Maggiore è questo numero, più velocemente l'applicazione verrà disinstallata, ma in questo caso il carico su Administration Server sarà più elevato.

- **Numero massimo di tentativi di disinstallazione**

  Se, durante l'esecuzione dell'attività *Disinstalla l'applicazione in remoto*, Kaspersky Security Center Linux non riesce a disinstallare un'applicazione in un dispositivo gestito entro il numero di esecuzioni del programma di installazione specificate dal parametro, Kaspersky Security Center Linux interrompe la distribuzione dell'utilità di disinstallazione a tale dispositivo gestito e non avvia più il programma di installazione nel dispositivo.

  Il parametro **Numero massimo di tentativi di disinstallazione** consente di salvare le risorse del dispositivo gestito, nonché di ridurre il traffico (disinstallazione, esecuzione del file MSI e messaggi di errore).

  I tentativi ricorrenti di avvio dell'attività possono indicare un problema nel dispositivo che impedisce la disinstallazione. L'amministratore dovrebbe risolvere il problema entro il numero specificato di tentativi di disinstallazione e quindi riavviare l'attività (manualmente o in base a una pianificazione).

  Se la disinstallazione non va a buon fine, il problema è ritenuto irrisolvibile e ulteriori tentativi di avvio dell'attività sono considerati dispendiosi in termini di risorse e traffico.

  Quando viene creata l'attività, il conteggio dei tentativi è impostato su `0`. Per ogni esecuzione del programma di installazione che restituisce un errore nel dispositivo il numero aumenta.

  Se il numero di tentativi specificati nel parametro è stato superato e il dispositivo è pronto per la disinstallazione dell'applicazione, è possibile aumentare il valore del parametro **Numero massimo di tentativi di disinstallazione** e avviare l'attività per disinstallare l'applicazione. In alternativa, è possibile creare una nuova attività *Disinstalla l'applicazione in remoto*.

- **Verifica il tipo di sistema operativo prima del download**

  Prima di trasmettere i file ai dispositivi client, Kaspersky Security Center Linux verifica se le impostazioni dell'utilità di installazione sono applicabili al sistema operativo del dispositivo client. Se le impostazioni non sono applicabili, Kaspersky Security Center Linux non trasmette i file e non tenta di installare l'applicazione. Ad esempio, per installare un'applicazione nei dispositivi di un gruppo di amministrazione che include dispositivi che eseguono vari sistemi operativi, è possibile assegnare l'attività di installazione al gruppo di amministrazione e quindi abilitare questa opzione per ignorare i dispositivi che eseguono un sistema operativo diverso da quello desiderato.

Procedere al passaggio successivo della procedura guidata.

9. Specificare le impostazioni per il riavvio del sistema operativo:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**
  - **Riavvia dopo (min.)**

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

  L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

  Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

  Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

  Per impostazione predefinita, questa opzione è disabilitata.

Procedere al passaggio successivo della procedura guidata.

10. Se necessario, aggiungere gli account che verranno utilizzati per avviare l'attività di disinstallazione remota:

- **Nessun account richiesto (Network Agent installato)**

  Se questa opzione è selezionata, non è necessario specificare un account con cui verrà eseguito il programma di installazione dell'applicazione. L'attività sarà eseguita tramite l'account con cui viene eseguito Administration Server.

  Se Network Agent non è stato installato nei dispositivi client, questa opzione non è disponibile.

- **Account richiesto (Network Agent non utilizzato)**

Selezionare questa opzione se Network Agent non è installato nei dispositivi a cui si assegna l'attività *Disinstalla l'applicazione in remoto*. In questo caso, è possibile specificare un account utente o un certificato SSH per disinstallare l'applicazione.

- **Account locale**. Se questa opzione è selezionata, specificare l'account utente con cui verrà eseguito il programma di installazione dell'applicazione. Fare clic sul pulsante **Aggiungi**, selezionare **Account locale** e quindi specificare le credenziali dell'account utente.

  È possibile specificare più account utente, ad esempio se nessuno di essi dispone di tutti i diritti richiesti per tutti i dispositivi per cui si assegna l'attività. In questo caso, tutti gli account aggiunti vengono utilizzati per l'esecuzione dell'attività, consecutivamente, dall'alto in basso.

- **Certificato SSH**. Se si desidera disinstallare un'applicazione da un dispositivo client basato su Linux, è possibile specificare un certificato SSH anziché un account utente. Fare clic sul pulsante **Aggiungi**, selezionare **Certificato SSH**, quindi specificare la chiave privata e quella pubblica del certificato.

  Per generare una chiave privata, è possibile utilizzare l'utilità ssh-keygen. Kaspersky Security Center Linux supporta il formato PEM delle chiavi private, ma l'utilità ssh-keygen genera chiavi SSH nel formato OPENSSH per impostazione predefinita. Il formato OPENSSH non è supportato da Kaspersky Security Center Linux. Per creare una chiave privata nel formato PEM supportato, aggiungere l'opzione -m PEM nel comando ssh-keygen.

  Ad esempio:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "< e-mail dell'utente >"
  ```

11. Nel passaggio **Completa creazione attività** della procedura guidata, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** per modificare le impostazioni predefinite dell'attività.

    Se non si abilita questa opzione, l'attività verrà creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in un secondo momento.

12. Fare clic sul pulsante **Fine**.

    La procedura guidata crea l'attività: Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata automaticamente la finestra delle proprietà dell'attività. In questa finestra, è possibile specificare le impostazioni generali dell'attività e, se necessario, modificare le impostazioni specificate durante la creazione dell'attività.

    È inoltre possibile aprire la finestra delle proprietà dell'attività facendo clic sul nome dell'attività creata nell'elenco delle attività.

    L'attività verrà creata, configurata e visualizzata nell'elenco delle attività in **Risorse (dispositivi)** → **Attività**.

13. Per eseguire l'attività, selezionarla nell'elenco delle attività, quindi fare clic sul pulsante **Avvia**.

    È inoltre possibile impostare una pianificazione per l'avvio dell'attività nella scheda **Pianificazione** della finestra delle proprietà dell'attività.

    Per una descrizione dettagliata delle impostazioni di avvio pianificato, fare riferimento alle impostazioni generali dell'attività.

Una volta completata l'attività, l'applicazione selezionata viene rimossa dai dispositivi selezionati.

Problemi di disinstallazione remota

A volte la disinstallazione remota di applicazioni di terze parti può terminare con il seguente avviso: "La disinstallazione remota è terminata su questo dispositivo con avvisi: l'applicazione per la rimozione delle applicazioni non è installata". Questo problema si verifica quando l'applicazione da disinstallare è già stata disinstallata o è stata installata solo per un singolo utente. Le applicazioni installate per un singolo utente (chiamate anche applicazioni per utente) diventano invisibili e non possono essere disinstallate da remoto se l'utente non ha effettuato l'accesso.

Questo comportamento è in contrasto con le applicazioni pensate per essere utilizzate da più utenti sullo stesso dispositivo (chiamate anche applicazioni per dispositivo). Le applicazioni per dispositivo sono visibili e accessibili a tutti gli utenti del dispositivo.

Pertanto, le applicazioni per utente devono essere disinstallate solo quando l'utente ha effettuato l'accesso.

Fonte di informazioni sulle applicazioni installate

Network Agent recupera informazioni sul software installato sui dispositivi Windows dalle seguenti chiavi di registro:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
  Contiene informazioni sulle applicazioni installate per tutti gli utenti.
- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall
  Contiene informazioni sulle applicazioni installate per tutti gli utenti.
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall
  Contiene informazioni sulle applicazioni installate per l'utente corrente.
- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall
  Contiene informazioni sulle applicazioni installate per utenti specifici.

Preparazione di un dispositivo che esegue SUSE Linux Enterprise Server 15 per l'installazione di Network Agent

Per installare Network Agent in un dispositivo con il sistema operativo SUSE Linux Enterprise Server 15:

Prima dell'installazione di Network Agent, eseguire il seguente comando:

```
$ sudo zypper install insserv-compat
```

Questo consente di installare il pacchetto insserv-compat e di configurare correttamente Network Agent.

Eseguire il comando `rpm -q insserv-compat` per verificare se il pacchetto è già installato.

Se la rete include molti dispositivi che eseguono SUSE Linux Enterprise Server 15, è possibile utilizzare il software apposito per la configurazione e la gestione dell'infrastruttura aziendale. Utilizzando questo software, è possibile installare automaticamente il pacchetto insserv-compat in tutti i dispositivi necessari contemporaneamente. È ad esempio possibile utilizzare Puppet, Ansible, Chef o è possibile creare il proprio script, usando il metodo più comodo.

Se il dispositivo non dispone delle chiavi di firma GPG per SUSE Linux Enterprise, è possibile che venga visualizzato il seguente avviso: `Package header is not signed!` Selezionare l'opzione `i` per ignorare l'avviso.

Dopo aver preparato il dispositivo SUSE Linux Enterprise Server 15, distribuire e installare Network Agent.

Preparazione di un dispositivo Windows per l'installazione remota

L'installazione remota dell'applicazione in un dispositivo client può restituire un errore per i seguenti motivi:

- L'attività è già stata eseguita nel dispositivo.

  In questo caso, non è necessario eseguire nuovamente l'attività.

- All'avvio di un'attività, il dispositivo era spento.

  In questo caso, accendere il dispositivo e avviare nuovamente l'attività.

- Non è stata stabilita la connessione tra l'Administration Server e il Network Agent installato nel dispositivo client.

  Per determinare la causa del problema, utilizzare l'utilità per la diagnostica remota dei dispositivi client (klactgui).

- Se nel dispositivo non è installato alcun Network Agent, durante l'installazione remota possono verificarsi i seguenti problemi:

  - Il dispositivo client ha l'opzione **Disattiva il Simple File Sharing** abilitata.
  - Il servizio Server non è in esecuzione nel dispositivo client.
  - Le porte richieste sono chiuse nel dispositivo client.
  - L'account utilizzato per l'esecuzione dell'attività dispone di privilegi insufficienti.

  Per evitare problemi che possono verificarsi durante l'installazione dell'applicazione in un dispositivo client senza Network Agent installato, è necessario procedere come descritto nella distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center Linux.

In precedenza, veniva utilizzata l'utilità riprep per preparare un dispositivo per l'installazione remota. Questo è ormai considerato un metodo obsoleto per la configurazione dei sistemi operativi. L'utilizzo dell'utilità riprep non è consigliabile nei sistemi operativi più recenti di Windows XP e Windows Server 2003 R2.

Preparazione di un dispositivo macOS per l'installazione remota di Network Agent

Per installare inizialmente Network Agent nel dispositivo gestito macOS, sono disponibili i seguenti metodi:

- Eseguendo l'attività di installazione remota nel punto di distribuzione macOS.
- Inviando agli utenti dei dispositivi collegamenti ai pacchetti indipendenti generati da Kaspersky Security Center Linux. I pacchetti indipendenti sono moduli eseguibili che contengono i pacchetti di distribuzione delle applicazioni selezionate con le relative impostazioni definite.

Per preparare un dispositivo macOS per l'installazione remota di Network Agent:

1. Accertarsi che Sudo sia installato nel dispositivo macOS di destinazione.

2. Testare la configurazione del dispositivo:

   a. Assicurarsi che la porta 22 sia aperta sul dispositivo client. A tale scopo, in **Preferenze di sistema**, aprire il riquadro **Condivisione**, quindi verificare che la casella di controllo **Accesso remoto** sia selezionata.

   È possibile connettersi al dispositivo client tramite Secure Shell (SSH) solo attraverso la porta 22. Non è possibile modificare il numero di porta.

   È possibile utilizzare il comando `ssh <nome_dispositivo>` per accedere in remoto al dispositivo macOS. Nel riquadro **Condivisione** è possibile utilizzare l'opzione **Consenti accesso per** per impostare l'ambito degli utenti a cui è consentito l'accesso al dispositivo macOS.

   b. Disabilitare la password sudo per l'account utente con cui deve essere eseguita la connessione del dispositivo.

   Utilizzare il comando `sudo visudo` in Terminale per aprire il file di configurazione sudoers. Nella voce `User privilege specification` del file aperto specificare quanto segue: `username ALL = (ALL) NOPASSWD: ALL`. In questo caso, `username` è l'account utente che deve essere utilizzato per la connessione del dispositivo tramite SSH.

   c. Salvare e chiudere il file sudoers.

   d. Eseguire di nuovo la connessione al dispositivo tramite SSH e verificare che il servizio Sudo non richieda l'immissione di una password. A tale scopo, utilizzare il comando `sudo whoami`.

3. Scaricare e creare un pacchetto di installazione:

   a. Scaricare il pacchetto di installazione di Network Agent utilizzando uno dei seguenti metodi:

   - Utilizzando l'interfaccia dell'applicazione
   - Scaricando la versione adeguata di Network Agent dal sito Web del Servizio di assistenza tecnica all'indirizzo https://support.kaspersky.com/
   - Richiedendo il pacchetto di installazione agli specialisti del Servizio di assistenza tecnica

   b. Per creare un pacchetto di installazione remota, utilizzare i seguenti file:

   - klnagent.kud
   - install.sh
   - klnagentmac.dmg

4. Crea un'attività di installazione remota con le seguenti impostazioni:

   - Nella pagina **Impostazioni** della Creazione guidata nuova attività, selezionare la casella di controllo **Utilizzando le risorse del sistema operativo tramite Administration Server**. Deselezionare tutte le altre caselle di controllo.
   - Nella pagina **Selezione di un account per l'esecuzione dell'attività** specificare le impostazioni dell'account utente utilizzato per la connessione del dispositivo tramite SSH.

Il dispositivo client è pronto per l'installazione remota di Network Agent tramite l'attività corrispondente che è stata creata.

Licensing

Questa scheda fornisce le seguenti informazioni:

- Concetti generali relativi alle licenze di Kaspersky Security Center Linux
- Istruzioni sulla gestione delle licenze delle applicazioni Kaspersky gestite

Licensing di Kaspersky Security Center Linux.

In questa sezione vengono descritti i concetti generali correlati alle licenze di Kaspersky Security Center Linux.

Informazioni sul Contratto di licenza con l'utente finale

Il *Contratto di licenza con l'utente finale* (Contratto di licenza o EULA) è un accordo vincolante tra l'utente e AO Kaspersky Lab, in cui sono definite le condizioni di utilizzo dell'applicazione.

Leggere attentamente il Contratto di licenza prima di iniziare a utilizzare l'applicazione.

Kaspersky Security Center Linux e i relativi componenti, ad esempio Network Agent, hanno Contratti di licenza con l'utente finale distinti.

È possibile visualizzare i termini del Contratto di licenza con l'utente finale per Kaspersky Security Center Linux utilizzando i seguenti metodi:

- Durante l'installazione di Kaspersky Security Center.
- Leggendo il documento license.txt incluso nel kit di distribuzione di Kaspersky Security Center.
- Leggendo il documento license. txt nella cartella di installazione di Kaspersky Security Center.
- Scaricando il file license.txt dal sito Web di Kaspersky.

È possibile visualizzare i termini del Contratto di licenza con l'utente finale per Network Agent per Linux utilizzando i seguenti metodi:

- Durante il download del pacchetto di distribuzione di Network Agent dai server Web di Kaspersky.
- Durante l'installazione di Network Agent per Linux.
- Leggendo il documento license.txt incluso nel pacchetto di distribuzione di Network Agent per Linux.
- Leggendo il documento license.txt nella cartella di installazione di Network Agent per Linux.
- Scaricando il file license.txt dal sito Web di Kaspersky.

Le condizioni del Contratto di licenza con l'utente finale si considerano accettate quando l'utente conferma l'accettazione del Contratto di licenza con l'utente finale durante l'installazione dell'applicazione. Se non si accettano le condizioni del Contratto di licenza, annullare l'installazione dell'applicazione e rinunciare all'utilizzo dell'applicazione.

Informazioni sulla licenza

Una *licenza* concede per un determinato periodo di tempo il diritto di utilizzare Kaspersky Security Center Linux, in conformità con i termini del Contratto di licenza (Contratto di licenza con l'utente finale).

L'ambito dei servizi forniti e il periodo di validità per l'utilizzo dell'applicazione dipendono dalla licenza utilizzata per attivare l'applicazione.

Sono disponibili i seguenti tipi di licenza:

- *Di prova*

  Una licenza gratuita che consente di valutare l'applicazione. Una licenza di prova ha in genere un periodo limitato.

  Alla scadenza di una licenza di prova, tutte le funzionalità di Kaspersky Security Center Linux vengono disabilitate. Per continuare a utilizzare l'applicazione, è necessario acquistare una licenza commerciale.

  È possibile utilizzare l'applicazione con una licenza di prova per un solo periodo di prova.

- *Commerciale*

  Una licenza a pagamento.

  Alla scadenza di una licenza commerciale, le funzionalità chiave dell'applicazione vengono disattivate. Per continuare a utilizzare Kaspersky Security Center, è necessario rinnovare la licenza commerciale. Dopo la scadenza di una licenza commerciale, non è possibile continuare a utilizzare l'applicazione ed è necessario rimuoverla dal dispositivo.

  È consigliabile rinnovare la licenza prima della scadenza per assicurare la protezione costante da tutti i tipi di minacce.

Informazioni sul certificato di licenza

Un *certificato di licenza* è un documento ricevuto insieme a un file chiave o a un codice di attivazione.

Un certificato di licenza contiene le seguenti informazioni sulla licenza fornita:

- Chiave di licenza o numero di ordine
- Informazioni sull'utente a cui è stata concessa la licenza
- Informazioni sull'applicazione che può essere attivata con la licenza fornita
- Limite del numero di unità di licensing (ad esempio dispositivi in cui può essere utilizzata l'applicazione con la licenza fornita)
- Data di inizio del periodo di validità della licenza
- Data di scadenza della licenza o periodo licenza
- Tipo di licenza

Informazioni sulla chiave di licenza

Una *chiave di licenza* è una sequenza di bit che è possibile applicare per attivare e quindi utilizzare l'applicazione in conformità alle condizioni del Contratto di licenza con l'utente finale. Le chiavi di licenza sono generate dagli specialisti di Kaspersky.

È possibile aggiungere una chiave di licenza all'applicazione utilizzando uno dei seguenti metodi: applicando un *file chiave* o inserendo un *codice di attivazione*. La chiave di licenza viene visualizzata nell'interfaccia dell'applicazione come sequenza alfanumerica univoca dopo essere stata aggiunta all'applicazione.

La chiave di licenza può essere bloccata da Kaspersky in caso di violazione delle condizioni del Contratto di licenza con l'utente finale. Se la chiave di licenza è stata bloccata, è necessario aggiungerne un'altra se si desidera utilizzare l'applicazione.

Una chiave di licenza può essere attiva o aggiuntiva (o di riserva).

Una *chiave di licenza attiva* è una chiave di licenza attualmente utilizzata dall'applicazione. È possibile aggiungere una chiave di licenza attiva per una licenza di prova o commerciale. L'applicazione non può avere più di una chiave di licenza attiva.

Una *chiave di licenza aggiuntiva (o di riserva)* è una chiave di licenza che concede all'utente il diritto di utilizzare l'applicazione, pur non essendo attualmente in uso. La chiave di licenza di riserva diventa automaticamente attiva alla scadenza della licenza associata alla chiave di licenza attiva corrente. Una chiave di licenza di riserva può essere aggiunta solo se è stata già aggiunta una chiave di licenza attiva.

Una chiave di licenza per una licenza di prova può essere aggiunta come chiave di licenza attiva. Non è possibile aggiungere come chiave di licenza di riserva una chiave di licenza per una licenza di prova.

Visualizzazione dell'Informativa sulla privacy

L'Informativa sulla privacy è disponibile online all'indirizzo https://www.kaspersky.com/products-and-services-privacy-policy.

L'Informativa sulla privacy è disponibile anche offline:

- È possibile consultare l'Informativa sulla privacy prima di installare Kaspersky Security Center Linux.
- Il testo dell'Informativa sulla privacy è incluso nel file license.txt, nella cartella di installazione di Kaspersky Security Center Linux.
- Il file privacy_policy.txt è disponibile in un dispositivo gestito, nella cartella di installazione di Network Agent.
- È possibile decomprimere il file privacy_policy.txt dal pacchetto di distribuzione di Network Agent.

Opzioni di licensing per Kaspersky Security Center

Kaspersky Security Center viene fornito insieme alle applicazioni Kaspersky per la protezione delle reti aziendali. Può inoltre essere scaricato dal sito Web di Kaspersky.

Utilizzando Kaspersky Security Center è possibile eseguire quanto segue:

- Creare una gerarchia di Administration Server per gestire la rete dell'organizzazione, nonché le reti di filiali remote o organizzazioni client.

  Un'*organizzazione client* è un'organizzazione la cui protezione anti-virus viene assicurata da un provider di servizi.

- Creare una gerarchia di gruppi di amministrazione per gestire una selezione di dispositivi client come una singola unità.
- Gestire un sistema di protezione anti-virus basato sulle applicazioni Kaspersky.
- Eseguire l'installazione remota delle applicazioni Kaspersky e di altri fornitori di software.
- Eseguire la distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky nei dispositivi client, monitorarne l'utilizzo e rinnovare le licenze.
- Ricevere statistiche e rapporti sull'esecuzione delle applicazioni e dei dispositivi.
- Ricevere notifiche relative agli eventi critici durante l'esecuzione delle applicazioni Kaspersky.
- Gestire il criptaggio delle informazioni archiviate in unità rimovibili e dischi rigidi di dispositivi basati su Windows.
- Gestire l'accesso degli utenti ai dati criptati nei dispositivi basati su Windows.
- Eseguire l'inventario dell'hardware connesso alla rete dell'organizzazione.
- Gestire in modo centralizzato il file spostati in Quarantena o Backup dalle applicazioni di protezione, nonché gestire i file per cui l'elaborazione da parte delle applicazioni di protezione è stata rimandata.

Informazioni sul file chiave

Un *file chiave* è un file con estensione key fornito all'utente da Kaspersky. I file chiave sono progettati per attivare l'applicazione attraverso l'aggiunta di una chiave di licenza.

Il file chiave viene ricevuto all'indirizzo e-mail specificato al momento dell'acquisto di Kaspersky Security Center o dell'ordine della versione di prova di Kaspersky Security Center.

Non è necessario connettersi ai server di attivazione di Kaspersky per attivare l'applicazione con un file chiave.

È possibile ripristinare un file chiave eliminato accidentalmente. Un file chiave potrebbe ad esempio essere necessario per eseguire la registrazione a Kaspersky CompanyAccount.

Per ripristinare il file chiave, eseguire una delle seguenti azioni:

- Contattare il venditore della licenza.
- Ricevere un file chiave tramite il sito Web di Kaspersky utilizzando il codice di attivazione disponibile.

Informazioni sulla trasmissione dei dati

Dati elaborati in locale

Kaspersky Security Center Linux è progettato per l'esecuzione centralizzata delle attività di base di amministrazione e manutenzione nella rete di un'organizzazione. Kaspersky Security Center Linux consente all'amministratore di accedere a informazioni dettagliate sul livello di protezione della rete dell'organizzazione; Kaspersky Security Center Linux consente a un amministratore di configurare tutti i componenti della protezione in base alle applicazioni Kaspersky. Kaspersky Security Center Linux esegue le seguenti funzioni principali:

- Rilevamento dei dispositivi e dei relativi utenti nella rete dell'organizzazione
- Creazione di una gerarchia di gruppi di amministrazione per la gestione dei dispositivi
- Installazione delle applicazioni Kaspersky nei dispositivi
- Gestione delle impostazioni e delle attività delle applicazioni installate
- Attivazione delle applicazioni Kaspersky nei dispositivi
- Gestione degli account utente
- Visualizzazione delle informazioni sul funzionamento delle applicazioni Kaspersky nei dispositivi
- Visualizzazione dei rapporti

Per eseguire le funzioni principali, Kaspersky Security Center Linux può ricevere, archiviare ed elaborare le seguenti informazioni:

- Informazioni sui dispositivi nella rete dell'organizzazione ricevute tramite la scansione dei controller di dominio Active Directory o Samba o tramite la scansione degli intervalli IP. Administration Server acquisisce i dati in modo indipendente o riceve i dati da Network Agent.
- Informazioni da Active Directory e Samba su unità organizzative, domini, utenti e gruppi. Administration Server ottiene i dati autonomamente o riceve i dati dal Network Agent assegnato come punto di distribuzione.
- Dettagli dei dispositivi gestiti. Network Agent trasferisce i dati elencati di seguito dal dispositivo ad Administration Server. L'utente inserisce il nome visualizzato e la descrizione del dispositivo nell'interfaccia di Kaspersky Security Center Web Console:
    - Specifiche tecniche del dispositivo gestito e relativi componenti richiesti per l'identificazione del dispositivo: nome visualizzato e descrizione del dispositivo, tipo e nome del dominio Windows (per i dispositivi appartenenti a un dominio Windows), nome del dispositivo nell'ambiente Windows (per i dispositivi appartenenti a un dominio Windows), dominio DNS e nome DNS, indirizzo IPv4, indirizzo IPv6, in posizione di rete, indirizzo MAC, tipo di sistema operativo, informazioni che indicano se il dispositivo è una macchina virtuale o meno e il tipo di hypervisor e informazioni che indicano se il dispositivo è una macchina virtuale dinamica nell'ambito di VDI.
    - Altre specifiche dei dispositivi gestiti e dei relativi componenti richieste per il controllo dei dispositivi gestiti: architettura del sistema operativo, vendor del sistema operativo, numero di build del sistema operativo, ID di rilascio del sistema operativo, cartella della posizione del sistema operativo; se il dispositivo è una macchina virtuale, il tipo di macchina virtuale e il nome dell'Administration Server virtuale che gestisce il dispositivo.
    - Dettagli delle azioni sui dispositivi gestiti: data e ora dell'ultimo aggiornamento, ora in cui il dispositivo è stato visibile per l'ultima volta nella rete, stato di attesa del riavvio e ora in cui il dispositivo è stato acceso.
    - Dettagli degli account utente del dispositivo e delle relative sessioni di lavoro.
- Dati ricevuti eseguendo la diagnostica remota in un dispositivo gestito: file di traccia, informazioni di sistema, dettagli delle applicazioni Kaspersky installate nel dispositivo, file di dump, registri eventi, risultati dell'esecuzione degli script di diagnostica ricevuti dall'Assistenza tecnica Kaspersky.

- Statistiche di funzionamento dei punti di distribuzione se il dispositivo è un punto di distribuzione. Network Agent trasferisce i dati dal dispositivo ad Administration Server.
- Impostazioni del punto di distribuzione immesse dall'utente in Kaspersky Security Center Web Console.
- Dettagli delle applicazioni Kaspersky installate nel dispositivo. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent:
  - Impostazioni delle applicazioni Kaspersky installate nel dispositivo gestito: nome e versione dell'applicazione Kaspersky, stato della protezione in tempo reale, data e ora dell'ultima scansione del dispositivo, numero delle minacce rilevate, numero di oggetti per i quali la disinfezione non è andata a buon fine, disponibilità e stato dei componenti dell'applicazione, dettagli delle attività e delle impostazioni delle applicazioni Kaspersky, informazioni sulla chiave di licenza attiva e su quella di riserva, ID e data di installazione dell'applicazione.
  - Statistiche sull'esecuzione dell'applicazione: eventi relativi alle modifiche dello stato dei componenti dell'applicazione Kaspersky nel dispositivo gestito e alle prestazioni delle attività avviate dai componenti dell'applicazione.
  - Stato del dispositivo definito dall'applicazione Kaspersky.
  - Tag assegnati dall'applicazione Kaspersky.
- Dati contenuti negli eventi dei componenti di Kaspersky Security Center Linux e delle applicazioni Kaspersky gestite. Network Agent trasferisce i dati dal dispositivo ad Administration Server.
- Impostazioni dei componenti Kaspersky Security Center Linux e delle applicazioni Kaspersky gestite presenti nei criteri e nei profili criterio. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.
- Impostazioni delle attività dei componenti Kaspersky Security Center Linux e delle applicazioni Kaspersky gestite. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.
- Dati elaborati dalla funzionalità di gestione del sistema. Network Agent trasferisce le seguenti informazioni dal dispositivo all'Administration Server:
  - Informazioni sull'hardware rilevato nei dispositivi gestiti (Registro hardware).

    Se Network Agent è installato in un dispositivo che esegue Windows, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo:

    - RAM
    - Dispositivi di archiviazione di massa
    - Scheda madre
    - CPU
    - Schede di rete
    - Monitor
    - Scheda video
    - Scheda audio

    Se Network Agent è installato in un dispositivo che esegue Linux, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo, se tali informazioni sono fornite dal sistema operativo:

    - Volume totale RAM
    - Volume totale dei dispositivi di archiviazione di massa
    - Scheda madre
    - CPU
    - Schede di rete
  - Informazioni relative al software installato nei dispositivi gestiti (registro software). Il software può essere confrontato con le informazioni sui file eseguibili rilevati nei dispositivi dalla funzione Controllo Applicazioni.
- Categorie utente di applicazioni. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.
- Elenco dei file eseguibili rilevati nei dispositivi gestiti dalla funzionalità Controllo Applicazioni. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.
- Informazioni sui dispositivi basati su Windows criptati e sullo stato di criptaggio. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent.
- Dettagli degli errori di criptaggio dei dati nei dispositivi basati su Windows utilizzando la funzionalità Criptaggio dei dati delle applicazioni Kaspersky. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.
- Dettagli dei file presenti in Backup. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.
- Dettagli dei file presenti in Quarantena. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.
- Dettagli dei file richiesti dagli specialisti Kaspersky per l'analisi dettagliata. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.
- Dettagli dei dispositivi esterni (unità di memoria, strumenti di trasferimento delle informazioni, strumenti HCRP informativi e bus di connessione) installati o connessi al dispositivo gestito e rilevati dalla funzionalità Controllo Dispositivi. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.
- Informazioni sui dispositivi criptati e sullo stato di criptaggio. Un'applicazione gestita trasferisce i dati dal dispositivo all'Administration Server tramite Network Agent.
- Informazioni sugli errori di criptaggio dei dati nei dispositivi. Il criptaggio viene eseguito dalla funzione Criptaggio dei dati delle applicazioni Kaspersky. Un'applicazione gestita trasferisce i dati dal dispositivo all'Administration Server tramite Network Agent. L'elenco completo di dati viene fornito nella Guida in linea dell'applicazione corrispondente.
- Elenco dei PLC (Programmable Logic Controller) gestiti. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Dati necessari per la creazione di una catena di sviluppo delle minacce. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Dettagli dei codici di attivazione immessi e dei file chiave immessi. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.

- Account utente: nome, descrizione, nome completo, indirizzo e-mail, numero di telefono principale e password. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Cronologia delle revisioni degli oggetti di gestione. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Registro degli oggetti di gestione dettagliati. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Pacchetti di installazione creati dal file, nonché impostazioni di installazione. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Dati necessari per la visualizzazione degli annunci di Kaspersky in Kaspersky Security Center Web Console. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Dati necessari per il funzionamento dei plug-in delle applicazioni gestite in Kaspersky Security Center Web Console e salvati dai plug-in nel database di Administration Server durante l'esecuzione standard. La descrizione e le modalità di invio dei dati sono specificate nei file della Guida dell'applicazione corrispondente.

- Impostazioni dell'utente di Kaspersky Security Center Web Console: lingua di localizzazione e tema dell'interfaccia, impostazioni di visualizzazione del riquadro Monitoraggio, informazioni sullo stato delle notifiche (Già letta/Non ancora letta), stato delle colonne nei fogli di calcolo (Mostra/Nascondi), avanzamento della modalità Training. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Certificato per la connessione sicura dei dispositivi gestiti ai componenti Kaspersky Security Center Linux. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Informazioni su quali termini dell'accordo legale di Kaspersky sono stati accettati dall'utente.

- I dati dell'Administration Server immessi dall'utente in Kaspersky Security Center Web Console o nell'interfaccia del programma Kaspersky Security Center OpenAPI.

- Tutti i dati che l'Utente immette nell'interfaccia di Kaspersky Security Center Web Console.

I dati elencati precedentemente possono essere presenti in Kaspersky Security Center Linux se viene applicato uno dei seguenti metodi:

- L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Network Agent riceve automaticamente i dati dal dispositivo e li trasferisce ad Administration Server.

- Network Agent riceve i dati recuperati dall'applicazione Kaspersky gestita e li trasferisce ad Administration Server. Gli elenchi dei dati elaborati dalle applicazioni Kaspersky gestite vengono forniti nei file della Guida per le applicazioni corrispondenti.

- Administration Server ottiene autonomamente le informazioni sui dispositivi in rete o riceve i dati dal Network Agent assegnato come punto di distribuzione.

I dati elencati vengono archiviati nel database di Administration Server. Nomi utente e password sono archiviati in formato criptato.

Tutti i dati elaborati localmente possono essere trasferiti a Kaspersky solo tramite file di dump, file di traccia o file di log dei componenti Kaspersky Security Center Linux, tra cui i file di log creati da strumenti di installazione e utilità.

I file di dump, i file di traccia o i file di log dei componenti di Kaspersky Security Center Linux contengono dati arbitrari di Administration Server, Network Agent e Kaspersky Security Center Web Console. I file possono contenere dati personali o riservati. I file di dump, i file di traccia o i file di log sono archiviati nel dispositivo in formato non criptato. I file di dump, i file di traccia o i file di log non vengono trasferiti automaticamente a Kaspersky, ma un amministratore può trasferire tali file su Kaspersky manualmente su richiesta dell'Assistenza tecnica per risolvere i problemi relativi alle prestazioni di Kaspersky Security Center Linux.

Kaspersky protegge le informazioni ricevute in conformità alle leggi e ai regolamenti applicabili di Kaspersky. I dati vengono trasmessi tramite un canale sicuro.

Seguendo i collegamenti in Administration Console o Kaspersky Security Center Web Console, l'Utente accetta di trasferire automaticamente i seguenti dati:

- Codice di Kaspersky Security Center Linux
- Versione di Kaspersky Security Center Linux
- Localizzazione di Kaspersky Security Center Linux
- ID licenza
- Tipo di licenza
- Se la licenza è stata acquistata tramite un partner

L'elenco dei dati forniti tramite ciascun collegamento dipende dalla finalità e dalla posizione del collegamento.

Kaspersky utilizza i dati ricevuti in forma anonima e soltanto come statistiche generali. Le statistiche riassuntive vengono generate automaticamente dalle informazioni ricevute in origine e non contengono dati personali o riservati. Non appena vengono accumulati nuovi dati, i dati precedenti vengono cancellati (una volta all'anno). Le statistiche riassuntive vengono archiviate a tempo indeterminato.

Informazioni sull'abbonamento

L'*abbonamento a Kaspersky Security Center Linux* è un ordine per l'utilizzo dell'applicazione con le impostazioni selezionate (data di scadenza dell'abbonamento, numero di dispositivi protetti). È possibile registrare l'abbonamento a Kaspersky Security Center Linux presso il provider di servizi (ad esempio il provider Internet). L'abbonamento può essere rinnovato manualmente o in modalità automatica; è possibile anche annullarlo.

Un abbonamento può essere limitato (ad esempio un anno) o illimitato (senza data di scadenza). Per continuare a utilizzare Kaspersky Security Center dopo la scadenza di un abbonamento limitato, è necessario rinnovarlo. L'abbonamento illimitato viene rinnovato automaticamente se il pagamento al provider di servizi è stato effettuato anticipatamente entro i termini.

Quando un abbonamento limitato scade, è possibile usufruire di un periodo di tolleranza per il rinnovo durante il quale l'applicazione continua a funzionare. La disponibilità e la durata del periodo di tolleranza sono definite dal provider di servizi.

Per utilizzare Kaspersky Security Center Linux con abbonamento, è necessario applicare il codice di attivazione ricevuto dal provider di servizi.

È possibile applicare un codice di attivazione diverso per Kaspersky Security Center Linux solo dopo la scadenza dell'abbonamento o in seguito all'annullamento.

A seconda del provider di servizi, il set di azioni possibili per la gestione dell'abbonamento può variare. Il provider di servizi potrebbe non fornire alcun periodo di tolleranza per il rinnovo dell'abbonamento, pertanto l'applicazione perde le funzionalità.

I codici di attivazione acquistati con l'abbonamento non possono essere utilizzati per attivare versioni precedenti di Kaspersky Security Center.

Quando si utilizza l'applicazione con abbonamento, Kaspersky Security Center Linux tenta automaticamente di accedere al server di attivazione a intervalli di tempo specificati fino alla scadenza dell'abbonamento. Se non è possibile accedere al server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici. È possibile rinnovare l'abbonamento nel sito Web del provider di servizi.

Attivazione di Kaspersky Security Center Linux

È possibile attivare Kaspersky Security Center Linux per utilizzare le funzionalità aggiuntive. Sono disponibili due modalità per eseguire questa attività: utilizzando l'Avvio rapido guidato di Administration Server o le proprietà di Administration Server.

Per attivare Kaspersky Security Center Linux:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Chiavi di licenza**.

3. In **Licenza corrente**, fare clic sul pulsante **Seleziona**.

4. Nella finestra visualizzata, selezionare la chiave di licenza che si desidera utilizzare per attivare Kaspersky Security Center Linux. Se la chiave di licenza non è elencata, fare clic sul pulsante **Aggiungi nuova chiave di licenza**, quindi specificare una nuova chiave di licenza.

5. Se necessario, è anche possibile aggiungere una chiave di licenza di riserva. A tale scopo, in **Chiave di licenza di riserva**, fare clic sul pulsante **Seleziona**, quindi selezionare una chiave di licenza esistente o aggiungerne una nuova. Si noti che non è possibile aggiungere una chiave di licenza di riserva se non è presente una chiave di licenza attiva.

6. Fare clic sul pulsante **Salva**.

Licensing delle applicazioni Kaspersky gestite

In questa sezione vengono descritte le funzionalità di Kaspersky Security Center relative all'utilizzo delle chiavi di licenza delle applicazioni Kaspersky gestite.

Kaspersky Security Center Linux consente la distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky nei dispositivi client, il monitoraggio del relativo utilizzo e il rinnovo delle licenze.

Quando si aggiunge una chiave di licenza utilizzando Kaspersky Security Center, le impostazioni della chiave di licenza vengono salvate nell'Administration Server. In base a queste informazioni, l'applicazione genera un rapporto sull'utilizzo delle chiavi di licenza e segnala all'amministratore la scadenza delle licenze e la violazione delle limitazioni di licenza specificate nelle proprietà delle chiavi di licenza. È possibile configurare le notifiche dell'utilizzo delle chiavi di licenza nelle impostazioni di Administration Server.

Licensing delle applicazioni gestite

Le applicazioni Kaspersky installate nei dispositivi gestiti devono essere concesse in licenza applicando un codice di attivazione o un file chiave a ognuna delle applicazioni. È possibile distribuire un codice di attivazione o un file chiave nei seguenti modi:

- Distribuzione automatica
- Il pacchetto di installazione di un'applicazione gestita
- Attività di aggiunta della chiave di licenza per un'applicazione gestita
- Attivazione manuale di un'applicazione gestita

È possibile aggiungere una nuova chiave di licenza attiva o di riserva con uno dei metodi sopra elencati. Un'applicazione Kaspersky utilizza una chiave attiva al momento e memorizza una chiave di riserva da applicare dopo la scadenza della chiave attiva. L'applicazione per la quale si aggiunge una chiave di licenza definisce se la chiave è attiva o aggiuntiva. La definizione della chiave non dipende dal metodo utilizzato per aggiungere una nuova chiave di licenza.

Distribuzione automatica

Se si utilizzano diverse applicazioni gestite ed è necessario distribuire un file chiave specifico o un codice di attivazione specifico nei dispositivi, valutare altre modalità di distribuzione del codice di attivazione o del file chiave in questione.

Kaspersky Security Center consente di distribuire automaticamente le chiavi di licenza disponibili nei dispositivi. Ad esempio, nell'archivio dell'Administration Server sono presenti tre chiavi di licenza. È stata abilitata l'opzione **Chiave di licenza distribuita automaticamente** per tutte e tre le chiavi di licenza. Un'applicazione di protezione Kaspersky, ad esempio Kaspersky Endpoint Security for Linux, è installata nei dispositivi dell'organizzazione. Viene rilevato un nuovo dispositivo a cui deve essere distribuita una chiave di licenza. L'applicazione stabilisce, ad esempio, che due delle chiavi di licenza dell'archivio possono essere distribuite al dispositivo: la chiave di licenza denominata *Key_1* e la chiave di licenza denominata *Key_2*. Una di queste chiavi di licenza viene distribuita nel dispositivo. In questo caso non è possibile prevedere quale delle due chiavi di licenza verrà distribuita nel dispositivo poiché la distribuzione automatica delle chiavi di licenza non offre nessuna attività di amministrazione.

Quando una chiave di licenza viene distribuita, i dispositivi vengono ricalcolati per questa chiave di licenza. È necessario accertarsi che il numero di dispositivi in cui è stata distribuita la chiave di licenza non superi la limitazione licenza. Se il numero di dispositivi supera la limitazione licenza, a tutti i dispositivi non coperti dalla licenza verrà assegnato lo stato *Critico*.

Prima della distribuzione, è necessario aggiungere il codice di attivazione o il file chiave all'archivio di Administration Server.

Istruzioni dettagliate:

- Aggiunta di una chiave di licenza all'archivio dell'Administration Server
- Distribuzione automatica di una chiave di licenza

Si noti che una chiave di licenza distribuita automaticamente potrebbe non essere visualizzata nell'archivio dell'Administration Server virtuale nei seguenti casi:

- La chiave di licenza non è valida per l'applicazione.
- L'Administration Server virtuale non dispone di dispositivi gestiti.
- La chiave di licenza è già stata utilizzata per i dispositivi sotto la gestione di un altro Administration Server virtuale ed è stato raggiunto il limite del numero di dispositivi.

Aggiunta di un file chiave o di un codice di attivazione al pacchetto di installazione di un'applicazione gestita

Per motivi di sicurezza, questa opzione non è consigliata. Un codice di attivazione o un file chiave di licenza aggiunto a un pacchetto di installazione può essere compromesso.

Se si installa un'applicazione gestita utilizzando un pacchetto di installazione, è possibile specificare un codice di attivazione o un file chiave nel pacchetto di installazione o nel criterio dell'applicazione. La chiave di licenza verrà distribuita nei dispositivi gestiti alla successiva sincronizzazione del dispositivo con Administration Server.

Istruzioni dettagliate: Aggiunta di una chiave di licenza a un pacchetto di installazione

Distribuzione tramite l'attività di aggiunta della chiave di licenza per un'applicazione gestita

Se si sceglie di utilizzare l'attività di aggiunta della chiave di licenza per un'applicazione gestita, è possibile selezionare la chiave di licenza che deve essere distribuita nei dispositivi e selezionare i dispositivi nella modalità più opportuna, ad esempio selezionando un gruppo di amministrazione o una selezione dispositivi.

Prima della distribuzione, è necessario aggiungere il codice di attivazione o il file chiave all'archivio di Administration Server.

Istruzioni dettagliate:

- Aggiunta di una chiave di licenza all'archivio dell'Administration Server
- Distribuzione di una chiave di licenza ai dispositivi client

Aggiunta manuale di un codice di attivazione o di un file chiave ai dispositivi

È possibile attivare l'applicazione Kaspersky installata in locale utilizzando gli strumenti disponibili nell'interfaccia dell'applicazione. Fare riferimento alla documentazione dell'applicazione installata.

Aggiunta di una chiave di licenza all'archivio dell'Administration Server

Per aggiungere una chiave di licenza all'archivio dell'Administration Server:

1. Nel menu principale, passare a **Operazioni** → **Licenze di Kaspersky**.
2. Fare clic sul pulsante **Aggiungi**.
3. Scegliere cosa si desidera aggiungere:
   - **Aggiungere un file chiave**

     Fare clic sul pulsante **Seleziona file chiave** e selezionare il file .key da aggiungere.
   - **Immettere il codice di attivazione**

     Specificare il codice di attivazione nel campo di testo e fare clic sul pulsante **Invia**.
4. Fare clic sul pulsante **Chiudi**.

Una o più chiavi di licenza verranno aggiunte all'archivio dell'Administration Server.

Distribuzione di una chiave di licenza ai dispositivi client

Kaspersky Security Center Web Console consente la distribuzione di una chiave di licenza ai dispositivi client automaticamente o tramite l'attività **Attivazione dell'applicazione**. È possibile utilizzare l'attività per distribuire le chiavi a un gruppo di dispositivi specifico. Durante la distribuzione di una chiave di licenza tramite l'attività, il limite di licenze relativo al numero di dispositivi non viene tenuto in considerazione. Utilizzare la distribuzione automatica delle chiavi per interrompere automaticamente la distribuzione di una chiave di licenza quando viene raggiunto il limite di licenze.

Se si abilita la distribuzione automatica di una chiave di licenza, non creare un'attività **Attivazione dell'applicazione** per distribuire tale chiave ai dispositivi client. In caso contrario, il carico su Administration Server aumenterà a causa della frequente sincronizzazione.

Prima della distribuzione, aggiungere una chiave di licenza all'archivio dell'Administration Server.

*Per distribuire una chiave di licenza ai dispositivi client tramite l'attività **Attivazione dell'applicazione**:*

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la **Creazione guidata nuova attività**. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Nell'elenco a discesa **Applicazione**, selezionare l'applicazione per la quale si desidera aggiungere una chiave di licenza.
4. Nell'elenco **Tipo di attività**, selezionare l'attività **Attivazione dell'applicazione**.
5. Nel campo **Nome attività**, specificare il nome della nuova attività.
6. Selezionare i dispositivi a cui verrà assegnata l'attività.
7. Nel passaggio **Selezione di una chiave di licenza** della procedura guidata, fare clic sul collegamento **Aggiungi chiave** per aggiungere la chiave di licenza.

8. Nel riquadro di aggiunta della chiave, aggiungere la chiave di licenza utilizzando una delle seguenti opzioni:

   È necessario aggiungere la chiave di licenza solo se non è stata aggiunta all'archivio dell'Administration Server prima di creare l'attività **Attivazione dell'applicazione**.

   - Selezionare l'opzione **Immettere il codice di attivazione** per immettere un codice di attivazione, quindi effettuare le seguenti operazioni:

     a. Specificare il codice di attivazione, quindi fare clic sul pulsante **Invia**.

        Le informazioni sulla chiave di licenza vengono visualizzate nel riquadro di aggiunta della chiave.

     b. Fare clic sul pulsante **Salva**.

        Se si desidera distribuire automaticamente la chiave di licenza ai dispositivi gestiti, abilitare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

        Il riquadro di aggiunta delle chiavi viene chiuso.

   - Selezionare l'opzione **Aggiungere un file chiave** per aggiungere un file chiave, quindi effettuare le seguenti operazioni:

     a. Fare clic sul pulsante **Seleziona file chiave**.

     b. Nella finestra visualizzata, selezionare un file chiave, quindi fare clic sul pulsante **Apri**.

        Le informazioni sulla chiave di licenza vengono visualizzate nel riquadro di aggiunta della chiave di licenza.

     c. Fare clic sul pulsante **Salva**.

        Se si desidera distribuire automaticamente la chiave di licenza ai dispositivi gestiti, abilitare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

        Il riquadro di aggiunta delle chiavi viene chiuso.

9. Selezionare la chiave di licenza nella tabella delle chiavi.

10. Nel passaggio **Informazioni sulla licenza** della procedura guidata, deselezionare la casella di controllo **Usa come chiave di riserva** predefinita se si desidera sostituire la chiave di licenza attiva.

    Ad esempio, questo è necessario quando l'organizzazione cambia ed è richiesta la chiave di un'altra organizzazione nel dispositivo o se la chiave è stata riemessa e una nuova licenza scade prima della licenza corrente. Per evitare errori, è necessario deselezionare la casella di controllo **Usa come chiave di riserva**.

    Per ulteriori informazioni sui problemi che possono verificarsi durante l'aggiunta di una chiave di licenza a Kaspersky Security Center e sui modi per risolverli, fare riferimento alla Knowledge Base di Kaspersky Security Center.

11. Nel passaggio **Completa creazione attività** della procedura guidata, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** per modificare le impostazioni predefinite dell'attività.

    Se non si abilita questa opzione, l'attività verrà creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in un secondo momento.

12. Fare clic sul pulsante **Fine**.

La procedura guidata crea l'attività: Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata automaticamente la finestra delle proprietà dell'attività. In questa finestra, è possibile specificare le impostazioni generali dell'attività e, se necessario, modificare le impostazioni specificate durante la creazione dell'attività.

> È inoltre possibile aprire la finestra delle proprietà dell'attività facendo clic sul nome dell'attività creata nell'elenco delle attività.

L'attività verrà creata, configurata e visualizzata nell'elenco delle attività.

13. Per eseguire l'attività, selezionarla nell'elenco delle attività, quindi fare clic sul pulsante **Avvia**.

    È inoltre possibile impostare una pianificazione per l'avvio dell'attività nella scheda **Pianificazione** della finestra delle proprietà dell'attività.

    Per una descrizione dettagliata delle impostazioni di avvio pianificato, fare riferimento alle impostazioni generali dell'attività.

Una volta completata l'attività, la chiave di licenza viene distribuita nei dispositivi selezionati.

Distribuzione automatica di una chiave di licenza

Kaspersky Security Center Linux consente la distribuzione automatica delle chiavi di licenza ai dispositivi gestiti, se sono presenti nell'archivio delle chiavi di licenza in Administration Server.

Per distribuire automaticamente una chiave di licenza ai dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.
2. Fare clic sul nome della chiave di licenza da distribuire automaticamente ai dispositivi.
3. Nella finestra delle proprietà della chiave di licenza visualizzata, selezionare la casella di controllo **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.
4. Fare clic sul pulsante **Salva**.

La chiave di licenza verrà automaticamente distribuita a tutti i dispositivi compatibili.

La distribuzione della chiave di licenza viene eseguita tramite Network Agent. Non vengono create attività di distribuzione della chiave di licenza per l'applicazione.

Durante la distribuzione automatica di una chiave di licenza, viene tenuto in considerazione il limite di licenze relativo al numero di dispositivi. Il limite di licenze è impostato nelle proprietà della chiave di licenza. Se viene raggiunto il limite di licenze, la distribuzione della chiave di licenza nei dispositivi si interrompe automaticamente.

Si noti che una chiave di licenza distribuita automaticamente potrebbe non essere visualizzata nell'archivio dell'Administration Server virtuale nei seguenti casi:

- La chiave di licenza non è valida per l'applicazione.
- L'Administration Server virtuale non dispone di dispositivi gestiti.

- La chiave di licenza è già stata utilizzata per i dispositivi sotto la gestione di un altro Administration Server virtuale ed è stato raggiunto il limite del numero di dispositivi.

L'Administration Server virtuale distribuisce automaticamente le chiavi di licenza dal proprio archivio e dall'archivio di Administration Server. È consigliabile:

- Utilizzare l'attività *Aggiungi chiave di licenza* per selezionare la chiave di licenza da distribuire nei dispositivi.

- Evitare di disabilitare l'opzione **Consenti la distribuzione automatica delle chiavi di licenza di questo Administration Server virtuale nei relativi dispositivi** nelle impostazioni dell'Administration Server virtuale. In caso contrario, l'Administration Server virtuale non distribuirà le chiavi di licenza ai dispositivi, comprese le chiavi di licenza dall'archivio di Administration Server.

Se si seleziona la casella di controllo **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti** nella finestra delle proprietà della chiave di licenza, nella rete viene immediatamente distribuita una chiave di licenza. Se non si seleziona questa opzione, è possibile utilizzare un'attività per distribuire una chiave di licenza in un secondo momento.

La distribuzione automatica delle chiavi di licenza configurate nell'Administration Server primario non si estende ai dispositivi gestiti da Administration Server secondari non virtuali.

Visualizzazione delle informazioni sulle chiavi di licenza in uso

Per visualizzare l'elenco delle chiavi di licenza aggiunte all'archivio di Administration Server:

Nel menu principale accedere a **Operazioni → Licensing → Licenze di Kaspersky**.

L'elenco visualizzato contiene i file chiave e i codici di attivazione aggiunti all'archivio di Administration Server.

Per visualizzare informazioni dettagliate su una chiave di licenza:

1. Nel menu principale accedere a **Operazioni → Licensing → Licenze di Kaspersky**.
2. Fare clic sul nome della chiave di licenza desiderata.

Nella finestra delle proprietà della chiave di licenza visualizzata è possibile visualizzare:

- Nella scheda **Generale**: le informazioni principali sulla chiave di licenza
- Nella scheda **Dispositivi**: l'elenco dei dispositivi client in cui è stata utilizzata la chiave di licenza per l'attivazione dell'applicazione Kaspersky installata

Per visualizzare quali chiavi di licenza sono distribuite in un dispositivo client specifico:

1. Nel menu principale accedere a **Risorse (dispositivi) → Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo desiderato.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Applicazioni**.
4. Fare clic sul nome dell'applicazione per cui si desidera visualizzare le informazioni sulla chiave di licenza.

5. Nella finestra delle proprietà dell'applicazione visualizzata, selezionare la scheda **Generale** e quindi aprire la sezione **Licenza**.

Verranno visualizzate le informazioni principali sulla chiave di licenza attiva e quella di riserva.

Per definire le impostazioni aggiornate delle chiavi di licenza dell'Administration Server virtuale, l'Administration Server invia una richiesta ai server di attivazione di Kaspersky almeno una volta al giorno. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici.

Eventi di superamento del limite di licenze

Kaspersky Security Center Linux consente di ottenere informazioni sugli eventi che si verificano in caso di superamento dei limiti di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client.

Il livello di importanza degli eventi quando avviene il superamento di un limite di licenze è definito in base alle regole seguenti:

- Se le unità attualmente in uso coperte da una singola licenza costituiscono tra il 90% e il 100% del numero totale di unità coperte dalla licenza, l'evento è pubblicato con il livello di importanza **Informazioni**.
- Se le unità attualmente in uso coperte da una singola licenza costituiscono tra il 100% e il 110% del numero totale di unità coperte dalla licenza, l'evento è pubblicato con il livello di importanza **Avviso**.
- Se il numero di unità attualmente in uso coperte da una singola licenza è superiore al 110% del numero totale di unità coperte dalla licenza, l'evento è pubblicato con il livello di importanza **Evento critico**.

Eliminazione di una chiave di licenza dall'archivio

Quando si elimina la chiave di licenza attiva distribuita in un dispositivo gestito, l'applicazione continuerà a funzionare sul dispositivo gestito.

Per eliminare un file chiave o un codice di attivazione dall'archivio di Administration Server:

1. Verificare che Administration Server non utilizzi un file chiave o un codice di attivazione che si desidera eliminare. In questo caso, non è possibile eliminare la chiave. Per eseguire il controllo:

   a. Nel menu principale, fare clic sull'icona delle impostazioni (🔧) accanto ad Administration Server.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

   b. Nella scheda **Generale** selezionare la sezione **Chiavi di licenza**.

   c. Se il file chiave o il codice di attivazione desiderato viene visualizzato nella sezione aperta, fare clic sul pulsante **Rimuovi chiave di licenza attiva**, quindi confermare l'operazione. Successivamente, Administration Server non utilizza la chiave di licenza eliminata, ma la chiave rimane nell'archivio dell'Administration Server. Se il file chiave o il codice di attivazione o desiderato non viene visualizzato, Administration Server non lo utilizza.

2. Nel menu principale accedere a **Operazioni → Licensing → Licenze di Kaspersky**.

3. Selezionare il file chiave o il codice di attivazione richiesti, quindi fare clic sul pulsante **Elimina**.

Il file chiave o il codice di attivazione selezionato verrà eliminato dall'archivio.

È possibile aggiungere nuovamente una chiave di licenza eliminata o aggiungerne una nuova.

Revoca del consenso a un Contratto di licenza con l'utente finale

Se si decide di interrompere la protezione di alcuni dispositivi client, è possibile revocare il Contratto di licenza con l'utente finale (EULA) per qualsiasi applicazione Kaspersky gestita. È necessario disinstallare l'applicazione selezionata prima di revocarne il Contratto di licenza con l'utente finale.

Per revocare un EULA per le applicazioni Kaspersky gestite:

1. Aprire la finestra delle proprietà di Administration Server e, nella scheda **Generale**, selezionare la sezione **Contratti di licenza con l'utente finale**.

   Verrà visualizzato un elenco degli EULA accettati al momento della creazione dei pacchetti di installazione, dell'installazione immediata degli aggiornamenti o della distribuzione di Kaspersky Security for Mobile.

2. Nell'elenco selezionare il Contratto di licenza con l'utente finale che si desidera revocare.

   È possibile visualizzare le seguenti proprietà degli EULA:

   - Data di accettazione del Contratto di licenza con l'utente finale
   - Nome dell'utente che ha accettato il Contratto di licenza con l'utente finale

3. Fare clic sulla data di accettazione di qualsiasi Contratto di licenza con l'utente finale per aprirne la finestra delle proprietà in cui sono visualizzati i seguenti dati:

   - Nome dell'utente che ha accettato il Contratto di licenza con l'utente finale
   - Data di accettazione del Contratto di licenza con l'utente finale
   - Identificatore univoco (UID) del Contratto di licenza con l'utente finale
   - Testo completo del Contratto di licenza con l'utente finale
   - Elenco di oggetti (pacchetti di installazione, aggiornamenti immediati, app mobili) collegati al Contratto di licenza con l'utente finale e relativi nomi e tipi

4. Nella parte inferiore della finestra delle proprietà del Contratto di licenza con l'utente finale fare clic sul pulsante **Revoca Contratto di licenza**.

   Se esistono oggetti (pacchetti di installazione e rispettive attività) che impediscono la revoca del Contratto di licenza con l'utente finale, viene visualizzata la notifica corrispondente. Non è possibile procedere con la revoca fino a quando non si eliminano questi oggetti.

   Nella finestra visualizzata l'utente viene informato della necessità di disinstallare prima l'applicazione Kaspersky corrispondente al Contratto di licenza con l'utente finale.

5. Fare clic sul pulsante per confermare la revoca.

L'EULA è revocato. Non viene più visualizzato nell'elenco dei Contratti di licenza nella sezione **Contratti di licenza con l'utente finale**. La finestra delle proprietà del Contratto di licenza con l'utente finale viene chiusa; l'applicazione non è più installata.

Rinnovo delle licenze per le applicazioni Kaspersky

È possibile rinnovare una licenza dell'applicazione Kaspersky scaduta o in scadenza (fra meno di 30 giorni).

Per rinnovare una licenza scaduta o una licenza che sta per scadere:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.
   - Nel menu principale, passare a **Monitoraggio e generazione dei rapporti** → **Dashboard**, quindi fare clic sul collegamento **View expiring licenses** accanto a una notifica.

   Verrà visualizzata la finestra **Licenze di Kaspersky** in cui è possibile visualizzare e rinnovare le licenze.

2. Fare clic sul collegamento **Rinnova licenza** accanto alla licenza richiesta.

   Facendo clic su un collegamento per il rinnovo della licenza l'utente accetta di trasferire a Kaspersky le seguenti informazioni su Kaspersky Security Center Linux: la versione, la localizzazione in uso, l'ID della licenza software (cioè l'ID della licenza per la quale si sta eseguendo il rinnovo) e se la licenza è stata acquistata tramite un'azienda partner o meno.

3. Nella finestra del servizio di rinnovo della licenza visualizzata seguire le istruzioni per rinnovare una licenza.

   La licenza viene rinnovata.

In Kaspersky Security Center Web Console le notifiche vengono visualizzate quando una licenza sta per scadere, in base alla seguente pianificazione:

- 30 giorni prima della scadenza
- 7 giorni prima della scadenza
- 3 giorni prima della scadenza
- 24 ore prima della scadenza
- Quando una licenza è scaduta

Utilizzo di Kaspersky Marketplace per scegliere le soluzioni aziendali Kaspersky

Marketplace è una sezione del menu principale che consente di visualizzare l'intera gamma di soluzioni aziendali Kaspersky, selezionare quelle desiderate e procedere all'acquisto nel sito Web di Kaspersky. È possibile utilizzare i filtri per visualizzare solo le soluzioni che si adattano alla propria organizzazione e ai requisiti del proprio sistema di sicurezza delle informazioni. Quando si seleziona una soluzione, Kaspersky Security Center Linux reindirizza alla relativa pagina Web nel sito Web di Kaspersky per ulteriori informazioni sulla soluzione. Ogni pagina Web consente di procedere all'acquisto o contiene istruzioni sulla procedura di acquisto.

Nella sezione **Marketplace** è possibile filtrare le soluzioni Kaspersky utilizzando i seguenti criteri:

- Numero di dispositivi (endpoint, server e altri tipi di asset) che si desidera proteggere:
  - 50–250
  - 250–1000
  - Più di 1000
- Livello di maturità del team di sicurezza delle informazioni dell'organizzazione:
  - **Foundations**

    Questo livello è tipico delle aziende che dispongono solo di un team IT. Il numero massimo di minacce possibili viene bloccato automaticamente.
  - **Optimum**

    Questo livello è tipico delle aziende che hanno una funzione di sicurezza IT specifica all'interno del team IT. A questo livello, le aziende richiedono soluzioni che consentano loro di contrastare le minacce commodity e le minacce che eludono i meccanismi di prevenzione esistenti.
  - **Expert**

    Questo livello è tipico delle aziende con ambienti IT complessi e distribuiti. Il team di sicurezza IT ha un livello di maturità ottimale o l'azienda dispone di un team SOC (Security Operations Center). Le soluzioni richieste consentono alle aziende di contrastare minacce complesse e attacchi mirati.
- Tipi di asset da proteggere:
  - **Endpoint**: workstation dei dipendenti, macchine fisiche e virtuali, sistemi integrati
  - **Server**: server fisici e virtuali
  - **Cloud**: ambienti cloud pubblici, privati o ibridi; servizi cloud
  - **Rete**: LAN, infrastruttura IT
  - **Servizio**: servizi relativi alla sicurezza forniti da Kaspersky

Per trovare e acquistare una soluzione aziendale Kaspersky:

1. Nel menu principale accedere a **Marketplace**.

   Per impostazione predefinita, la sezione mostra tutte le soluzioni aziendali Kaspersky disponibili.
2. Per visualizzare solo le soluzioni adatte alla propria organizzazione, selezionare i valori desiderati nei filtri.
3. Fare clic sulla soluzione che si desidera acquistare o per cui si desidera ottenere maggiori informazioni.

Si verrà reindirizzati alla pagina Web della soluzione. È possibile seguire le istruzioni visualizzate per procedere all'acquisto.

Configurazione delle applicazioni Kaspersky

Questa sezione contiene informazioni sulla configurazione manuale di criteri e attività, sui ruoli utente, sulla creazione di una struttura di gruppi di amministrazione e sulla gerarchia delle attività.

Scenario: Configurazione della protezione di rete

L'avvio rapido guidato crea criteri e attività con le impostazioni predefinite. Queste impostazioni possono risultare non ottimali o addirittura non consentite da un'organizzazione. Pertanto, è consigliabile ottimizzare tali criteri e attività, quindi creare altri criteri e attività, se necessario per la rete.

Prerequisiti

Prima di iniziare, verificare di avere:

- Installato Kaspersky Security Center Linux Administration Server
- Installato Kaspersky Security Center Web Console
- completato lo scenario di installazione principale di Kaspersky Security Center Linux
- completato l'Avvio rapido guidato o creato manualmente i seguenti criteri e attività nel gruppo di amministrazione **Dispositivi gestiti**:
  - Criterio di Kaspersky Endpoint Security
  - Attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
  - Criterio di Network Agent

Passaggi

La configurazione della protezione della rete procede per fasi:

1. **Installazione e propagazione dei criteri e dei profili criterio delle applicazioni Kaspersky**

   Per configurare e propagare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti, è possibile utilizzare due diversi metodi di gestione della protezione: quello incentrato sui dispositivi o quello incentrato sugli utenti. Questi due metodi possono essere combinati.

2. **Configurazione delle attività per la gestione remota delle applicazioni Kaspersky**

   Controllare le attività create con l'avvio rapido guidato e, se necessario, ottimizzarle.

   Istruzioni dettagliate: Configurazione dell'attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security

   Se necessario, creare attività aggiuntive per gestire le applicazioni Kaspersky installate nei dispositivi client.

3. **Valutazione e limitazione del carico di eventi nel database**

   Le informazioni sugli eventi che si verificano durante il funzionamento delle applicazioni gestite vengono trasferite da un dispositivo client e registrate nel database di Administration Server. Per ridurre il carico su Administration Server, valutare e limitare il numero massimo di eventi che possono essere archiviati nel database.

Istruzioni dettagliate: Impostazione del numero massimo di eventi

Risultati

Quando viene completato questo scenario, la rete sarà protetta tramite la configurazione delle applicazioni Kaspersky, delle attività e degli eventi ricevuti da parte di Administration Server:

- Le applicazioni Kaspersky sono configurate in base ai criteri e ai profili criterio.
- Le applicazioni vengono gestite attraverso un set di attività.
- Viene impostato il numero massimo di eventi che è possibile archiviare nel database.

Al termine della configurazione della protezione di rete, è possibile procedere alla configurazione degli aggiornamenti standard nei database e nelle applicazioni Kaspersky.

Informazioni sui metodi di gestione della protezione incentrati sui dispositivi e incentrati sugli utenti

È possibile gestire le impostazioni di protezione dal punto di vista delle funzionalità del dispositivo e dal punto di vista dei ruoli utente. Il primo metodo è denominato *gestione della protezione incentrata sui dispositivi* e il secondo è denominato *gestione della protezione incentrata sugli utenti*. Per applicare impostazioni dell'applicazione diverse a diversi dispositivi è possibile utilizzare uno o entrambi i tipi di gestione insieme.

La gestione della protezione incentrata sui dispositivi consente di applicare diverse impostazioni dell'applicazione di protezione ai dispositivi gestiti in base alle funzionalità specifiche del dispositivo. È ad esempio possibile applicare impostazioni diverse ai dispositivi allocati in diversi gruppi di amministrazione.

La gestione della protezione incentrata sugli utenti consente di applicare diverse impostazioni dell'applicazione di protezione a diversi ruoli utente. È possibile creare diversi ruoli utente, assegnare un ruolo utente appropriato a ciascun utente e definire diverse impostazioni dell'applicazione per i dispositivi di proprietà di utenti con ruoli diversi. È ad esempio possibile applicare differenti impostazioni dell'applicazione ai dispositivi degli addetti alla contabilità e degli specialisti delle risorse umane (HR). Di conseguenza, quando viene implementata la gestione della protezione incentrata sugli utenti, ciascun reparto (reparto account e reparto HR) dispone della propria configurazione delle impostazioni per le applicazioni Kaspersky. Una configurazione delle impostazioni definisce le impostazioni delle applicazioni che possono essere modificate dagli utenti e quelle che vengono forzatamente impostate e bloccate dall'amministratore.

Utilizzando la gestione della protezione incentrata sugli utenti è possibile applicare impostazioni specifiche di un'applicazione per singoli utenti. Questo può essere necessario quando un dipendente ha un ruolo esclusivo nell'azienda o quando si desidera monitorare i problemi di sicurezza relativi ai dispositivi di una persona specifica. A seconda del ruolo di questo dipendente nell'azienda, è possibile espanderne o limitarne i diritti di modifica delle impostazioni dell'applicazione. È ad esempio possibile espandere i diritti di un amministratore di sistema che gestisce i dispositivi client in una sede locale.

È inoltre possibile combinare gli approcci di gestione della protezione incentrata sui dispositivi e incentrata sugli utenti. È ad esempio possibile configurare uno specifico criterio dell'applicazione per ogni gruppo di amministrazione e quindi creare profili criterio per uno o più ruoli utente dell'azienda. In questo caso criteri e profili criterio vengono applicati nel seguente ordine:

1. Vengono applicati i criteri creati per la gestione della protezione incentrata sui dispositivi.
2. Questi vengono modificati dai profili criterio secondo le priorità dei profili criterio.

3. I criteri vengono modificati dai profili criterio associati ai ruoli utente.

Configurazione e propagazione dei criteri: approccio incentrato sui dispositivi

Al termine di questo scenario, le applicazioni saranno configurate in tutti i dispositivi gestiti in base ai criteri delle applicazioni e ai profili criterio specificati.

Prerequisiti

Prima di iniziare, verificare di aver installato Kaspersky Security Center Linux Administration Server e Kaspersky Security Center Web Console. È inoltre possibile valutare la gestione della protezione incentrata sull'utente come opzione alternativa o aggiuntiva all'approccio incentrato sui dispositivi. Ulteriori informazioni sui due approcci di gestione.

Passaggi

Lo scenario di gestione incentrata sui dispositivi delle applicazioni Kaspersky comprende i seguenti passaggi:

1. **Configurazione dei criteri delle applicazioni**

   Configurare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti tramite la creazione di un criterio per ogni applicazione. Questo set di criteri sarà propagato ai dispositivi client.

   Quando si configura la protezione della rete in Avvio rapido guidato, Kaspersky Security Center Linux crea il criterio predefinito per le seguenti applicazioni:

   - Kaspersky Endpoint Security for Linux: per dispositivi client basati su Linux
   - Kaspersky Endpoint Security for Windows: per dispositivi client basati su Windows

   Se è stata completata la configurazione tramite questa procedura guidata, non è necessario creare un nuovo criterio per questa applicazione.

   Se si dispone di una struttura gerarchica con più Administration Server e/o gruppi di amministrazione, per impostazione predefinita gli Administration Server secondari e i gruppi di amministrazione figlio ereditano i criteri dall'Administration Server primario. È possibile forzare l'ereditarietà da parte dei gruppi figlio e degli Administration Server secondari per impedire eventuali modifiche delle impostazioni configurate nel criterio upstream. Se si desidera forzare l'ereditarietà solo di una parte delle impostazioni, è possibile bloccarle nel criterio upstream. Le restanti impostazioni sbloccate saranno disponibili per la modifica nei criteri downstream. La gerarchia di criteri creata consente di gestire in modo efficace i dispositivi nei gruppi di amministrazione.

   Istruzioni dettagliate: Creazione di un criterio

2. **Creazione dei profili criterio (facoltativo)**

   Se si desidera applicare differenti impostazioni dei criteri ai dispositivi all'interno di un singolo gruppo di amministrazione, creare profili criterio per tali dispositivi. Un profilo criterio è un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita *condizione di attivazione del profilo*. I profili contengono solo le impostazioni diverse dal criterio "di base" che è attivo nel dispositivo gestito.

Utilizzando le condizioni di attivazione del profilo, è possibile applicare diversi profili criterio, ad esempio ai dispositivi con una specifica configurazione hardware o contrassegnati con tag specifici. Utilizzare i tag per filtrare i dispositivi che soddisfano i criteri specificati. È ad esempio possibile creare un tag denominato *CentOS*, contrassegnare tutti i dispositivi con sistema operativo CentOS con questo tag e quindi specificare il tag come condizione di attivazione per un profilo criterio. Come risultato, le applicazioni Kaspersky installate in tutti i dispositivi che eseguono CentOS verranno gestite dal profilo criterio corrispondente.

Istruzioni dettagliate:

- Creazione di un profilo criterio
- Creazione di una regola di attivazione del profilo criterio

3. **Propagazione di criteri e profili criterio nei dispositivi gestiti**

   Per impostazione predefinita, Administration Server si sincronizza automaticamente con i dispositivi gestiti ogni 15 minuti. Durante la sincronizzazione, i criteri e i profili criterio nuovi o modificati vengono propagati ai dispositivi gestiti. È possibile ignorare la sincronizzazione automatica ed eseguire manualmente la sincronizzazione utilizzando il comando Forza sincronizzazione. Al termine della sincronizzazione, i criteri e i profili criterio vengono inviati e applicati alle applicazioni Kaspersky installate.

   È possibile verificare se i criteri e i profili criterio sono stati distribuiti a un dispositivo. Kaspersky Security Center Linux specifica la data e l'ora di invio nelle proprietà del dispositivo.

   Istruzioni dettagliate: Sincronizzazione forzata

Risultati

Al termine dello scenario incentrato sui dispositivi, le applicazioni Kaspersky vengono configurate in base alle impostazioni specificate e propagate tramite la gerarchia di criteri.

I criteri delle applicazioni e i profili criterio configurati verranno applicati automaticamente ai nuovi dispositivi aggiunti ai gruppi di amministrazione.

Configurazione e propagazione dei criteri: approccio incentrato sull'utente

Questa sezione descrive lo scenario relativo all'approccio incentrato sugli utenti alla configurazione centralizzata delle applicazioni Kaspersky installate nei dispositivi gestiti. Al termine di questo scenario, le applicazioni saranno configurate in tutti i dispositivi gestiti in base ai criteri delle applicazioni e ai profili criterio specificati.

Prerequisiti

Prima di iniziare, verificare di aver installato correttamente Kaspersky Security Center Linux Administration Server e Kaspersky Security Center Web Console e completato lo scenario di distribuzione principale. È inoltre possibile valutare la gestione della protezione incentrata sui dispositivi come opzione alternativa o aggiuntiva all'approccio incentrato sugli utenti. Ulteriori informazioni sui due approcci di gestione.

Processo

Lo scenario di gestione incentrata sugli utenti delle applicazioni Kaspersky comprende i seguenti passaggi:

1. **Configurazione dei criteri delle applicazioni**

Configurare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti tramite la creazione di un criterio per ogni applicazione. Questo set di criteri sarà propagato ai dispositivi client.

Quando si configura la protezione della rete in avvio rapido guidato, Kaspersky Security Center Linux crea il criterio predefinito per Kaspersky Endpoint Security. Se è stata completata la configurazione tramite questa procedura guidata, non è necessario creare un nuovo criterio per questa applicazione.

Se si dispone di una struttura gerarchica con più Administration Server e/o gruppi di amministrazione, per impostazione predefinita gli Administration Server secondari e i gruppi di amministrazione figlio ereditano i criteri dall'Administration Server primario. È possibile forzare l'ereditarietà da parte dei gruppi figlio e degli Administration Server secondari per impedire eventuali modifiche delle impostazioni configurate nel criterio upstream. Se si desidera forzare l'ereditarietà solo di una parte delle impostazioni, è possibile bloccarle nel criterio upstream. Le restanti impostazioni sbloccate saranno disponibili per la modifica nei criteri downstream. La gerarchia di criteri creata consente di gestire in modo efficace i dispositivi nei gruppi di amministrazione.

Istruzioni dettagliate: Creazione di un criterio

2. **Specificazione dei proprietari dei dispositivi**

   Assegnare i dispositivi gestiti agli utenti corrispondenti.

   Istruzioni dettagliate: Assegnazione di un utente come proprietario dispositivo

3. **Definizione dei ruoli utente tipici dell'azienda**

   Prendere in considerazione i diversi tipi di attività eseguite dai dipendenti dell'azienda. È necessario suddividere tutti i dipendenti in base ai rispettivi ruoli. È ad esempio possibile suddividerli per reparto, professioni o posizioni. A questo punto, sarà necessario creare un ruolo utente per ciascun gruppo. Tenere presente che ogni ruolo utente avrà uno specifico profilo criterio che contiene le impostazioni delle applicazioni specifiche per questo ruolo.

4. **Creazione dei ruoli utente**

   Creare e configurare un ruolo utente per ogni gruppo di dipendenti che è stato definito nel passaggio precedente o utilizzare i ruoli utente predefiniti. I ruoli utente conterranno set di diritti di accesso alle funzionalità dell'applicazione.

   Istruzioni dettagliate: Creazione di un ruolo utente

5. **Definizione dell'ambito di ogni ruolo utente**

   Per ognuno dei ruoli utente creati, definire gli utenti e/o i gruppi di protezione e i gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

   Istruzioni dettagliate: Modifica dell'ambito di un ruolo utente

6. **Creazione di profili criterio**

   Creare un profilo criterio per ogni ruolo utente nell'organizzazione. I profili criterio definiscono le impostazioni che saranno applicate alle applicazioni installate nei dispositivi degli utenti, a seconda del ruolo di ogni utente.

   Istruzioni dettagliate: Creazione di un profilo criterio

7. **Associazione dei profili criterio ai ruoli utente**

   Associare i profili criterio creati ai ruoli utente. In tal modo, il profilo criterio diventa attivo per un utente che ha il ruolo specificato. Le impostazioni configurate nel profilo criterio verranno applicate alle applicazioni Kaspersky installate nei dispositivi dell'utente.

   Istruzioni dettagliate: Associazione dei profili criterio ai ruoli

8. **Propagazione di criteri e profili criterio nei dispositivi gestiti**

Per impostazione predefinita, Kaspersky Security Center Linux sincronizza automaticamente l'Administration Server con i dispositivi gestiti ogni 15 minuti. Durante la sincronizzazione, i criteri e i profili criterio nuovi o modificati vengono propagati ai dispositivi gestiti. È possibile ignorare la sincronizzazione automatica ed eseguire manualmente la sincronizzazione utilizzando il comando Forza sincronizzazione. Al termine della sincronizzazione, i criteri e i profili criterio vengono inviati e applicati alle applicazioni Kaspersky installate.

È possibile verificare se i criteri e i profili criterio sono stati distribuiti a un dispositivo. Kaspersky Security Center Linux specifica la data e l'ora di invio nelle proprietà del dispositivo.

Istruzioni dettagliate: Sincronizzazione forzata

Risultati

Al termine dello scenario incentrato sugli utenti, le applicazioni Kaspersky vengono configurate in base alle impostazioni specificate e propagate tramite la gerarchia di criteri e profili criterio.

Per un nuovo utente, sarà necessario creare un nuovo account e quindi assegnare all'utente uno dei ruoli utente creati e i dispositivi. I criteri delle applicazioni e i profili criterio configurati verranno applicati automaticamente ai dispositivi di questo utente.

Criteri e profili criterio

In Kaspersky Security Center Web Console è possibile creare criteri per le applicazioni Kaspersky. Questa sezione descrive i criteri e i profili criterio e fornisce istruzioni per crearli e modificarli.

Informazioni su criteri e profili criterio

Un *criterio* è un set di impostazioni dell'applicazione Kaspersky che vengono applicate a un gruppo di amministrazione e ai relativi sottogruppi. È possibile installare diverse applicazioni Kaspersky nei dispositivi di un gruppo di amministrazione. Kaspersky Security Center fornisce un singolo criterio per ogni applicazione Kaspersky in un gruppo di amministrazione. Un criterio può avere uno dei seguenti stati:

Lo stato del criterio

Stato	Descrizione
Attivo	Il criterio corrente applicato al dispositivo. Può essere attivo un solo criterio per un'applicazione Kaspersky in ogni gruppo di amministrazione. I dispositivi applicano i valori delle impostazioni di un criterio attivo per un'applicazione Kaspersky.
Inattivo	Un criterio che non è attualmente applicato a un dispositivo.
Fuori sede	Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.

I criteri funzionano secondo le seguenti regole:

- È possibile configurare diversi criteri con differenti impostazioni per una singola applicazione.
- Un solo criterio può essere attivo per l'applicazione corrente.
- Un criterio può avere criteri secondari.

In generale è possibile utilizzare i criteri in preparazione a situazioni di emergenza, come un attacco virus. Ad esempio in caso di attacco tramite unità flash, è possibile attivare un criterio che blocca l'accesso alle unità flash. In questo caso il criterio attivo corrente diventa automaticamente inattivo.

Per evitare di dover gestire più criteri, ad esempio quando diverse occasioni presuppongono solo la modifica di più impostazioni, è possibile utilizzare i profili criterio.

Un *profilo criterio* è un sottoinsieme denominato di valori delle impostazioni dei criteri che sostituisce i valori delle impostazioni di un criterio. Un profilo criterio influisce sulla creazione delle impostazioni ottimizzate in un dispositivo gestito. Per *impostazioni effettive* si intende un insieme di impostazioni dei criteri, impostazioni dei profili criterio e impostazioni delle applicazioni locali attualmente applicate nel dispositivo.

I profili criterio funzionano secondo le seguenti regole:

- Un profilo criterio assume validità quando si verifica una condizione di attivazione specifica.
- I profili criterio contengono valori delle impostazioni che differiscono dalle impostazioni dei criteri.
- L'attivazione di un profilo criterio modifica le impostazioni effettive del dispositivo gestito.
- Un criterio può includere al massimo 100 profili criterio.

Informazioni su blocco e impostazioni bloccate

Ogni impostazione dei criteri ha un'icona a forma di lucchetto (). La tabella seguente mostra gli stati dei pulsanti a forma di lucchetto:

Stati dei pulsanti a forma di lucchetto

Stato	Descrizione
Indefinito	Se accanto a un'impostazione viene visualizzato un lucchetto aperto e l'interruttore è disabilitato, l'impostazione non è specificata nel criterio. Un utente può modificare queste impostazioni nell'interfaccia dell'applicazione gestita. Questa tipologia di impostazioni è denominata *sbloccata*.
Applica	Se accanto a un'impostazione viene visualizzato un lucchetto chiuso e l'interruttore è abilitato, l'impostazione viene applicata ai dispositivi ai quali si applica il criterio. Un utente non può modificare i valori di queste impostazioni nell'interfaccia dell'applicazione gestita. Questa tipologia di impostazioni è denominata *bloccata*.

È consigliabile bloccare le impostazioni dei criteri che si desidera applicare ai dispositivi gestiti. Le impostazioni dei criteri sbloccate possono essere riassegnate dalle impostazioni dell'applicazione Kaspersky in un dispositivo gestito.

È possibile utilizzare un pulsante a forma di lucchetto per eseguire le seguenti azioni:

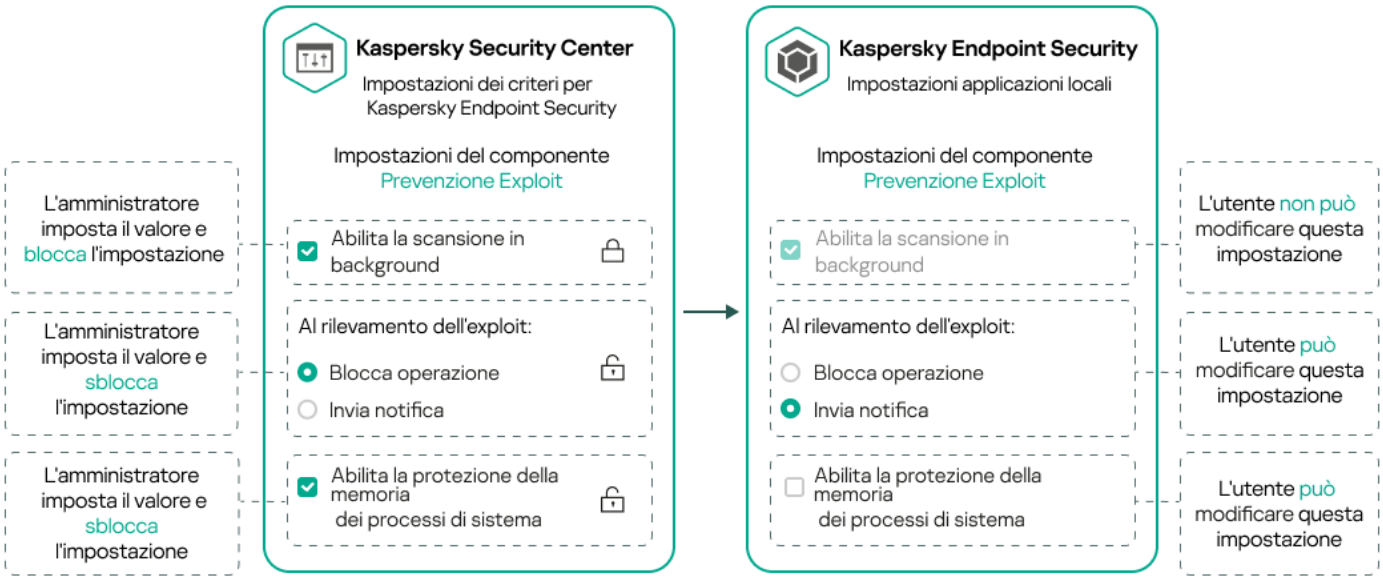
- Blocco delle impostazioni per il criterio di un sottogruppo di amministrazione
- Blocco delle impostazioni di un'applicazione Kaspersky in un dispositivo gestito

Un'impostazione bloccata viene pertanto utilizzata per implementare impostazioni ottimizzate in un dispositivo gestito.

Un processo di implementazione delle impostazioni ottimizzate include le seguenti azioni:

- Il dispositivo gestito applica i valori delle impostazioni dell'applicazione Kaspersky.
- Il dispositivo gestito applica i valori delle impostazioni bloccate di un criterio.

Un criterio e un'applicazione Kaspersky gestita contengono lo stesso set di impostazioni. Quando si configurano le impostazioni dei criteri, le impostazioni dell'applicazione Kaspersky assumono valori differenti in un dispositivo gestito. Non è possibile regolare le impostazioni bloccate in un dispositivo gestito (vedere la figura seguente):



Blocchi e impostazioni delle applicazioni Kaspersky

Ereditarietà di criteri e profili criterio

Questa sezione fornisce informazioni sulla gerarchia e sull'ereditarietà dei criteri e dei profili criterio.

Gerarchia dei criteri

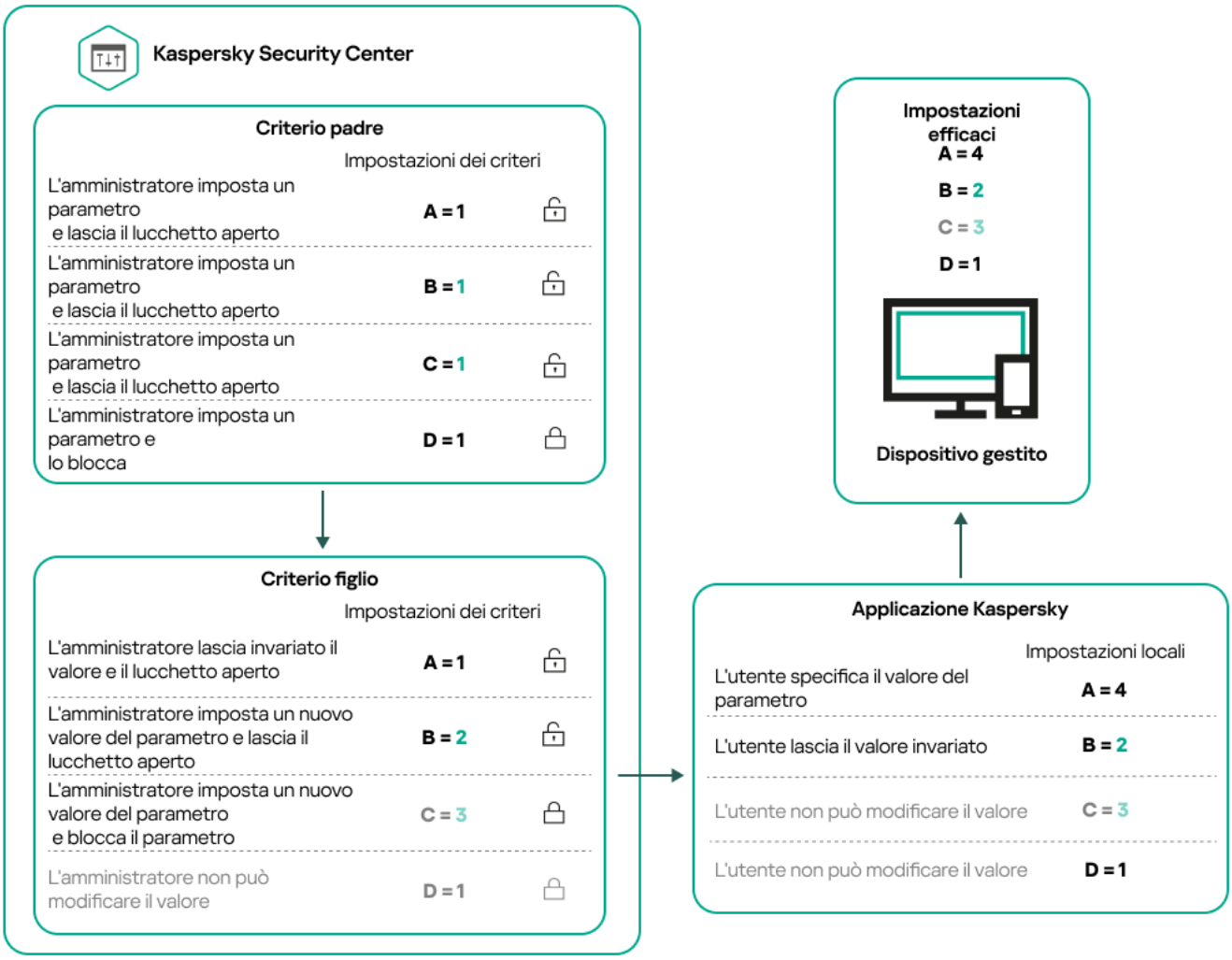
Se dispositivi diversi richiedono impostazioni diverse, è possibile organizzare i dispositivi in gruppi di amministrazione.

È possibile specificare un criterio per un singolo gruppo di amministrazione. Le impostazioni dei criteri possono essere *ereditate*. Ereditarietà significa ricevere i valori delle impostazioni dei criteri nei sottogruppi (gruppi secondari) di un criterio di un gruppo di amministrazione (principale) di livello superiore.

Da questo momento in poi, un criterio per un gruppo padre viene denominato anche *criterio principale*. Un criterio per un sottogruppo (gruppo figlio) viene inoltre denominato *criterio secondario*.

Per impostazione predefinita, esiste almeno un gruppo di dispositivi gestiti in Administration Server. Se si desidera creare gruppi personalizzati, questi vengono creati come sottogruppi (gruppi figlio) all'interno del gruppo di dispositivi gestiti.

I criteri della stessa applicazione si influenzano reciprocamente in base a una gerarchia di gruppi di amministrazione. Le impostazioni bloccate di un criterio di un gruppo di amministrazione di livello superiore (padre) riassegneranno i valori delle impostazioni dei criteri di un sottogruppo (vedere la figura seguente).

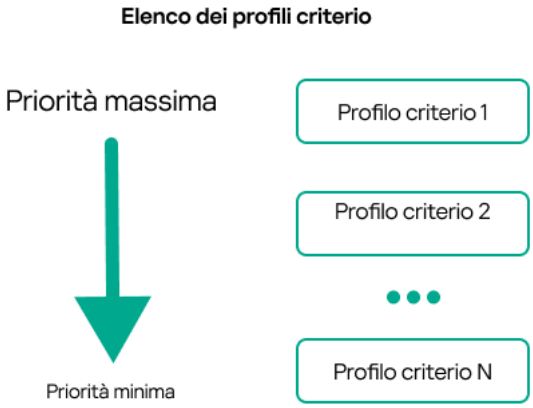


Gerarchia dei criteri

Profili criterio in una gerarchia di criteri

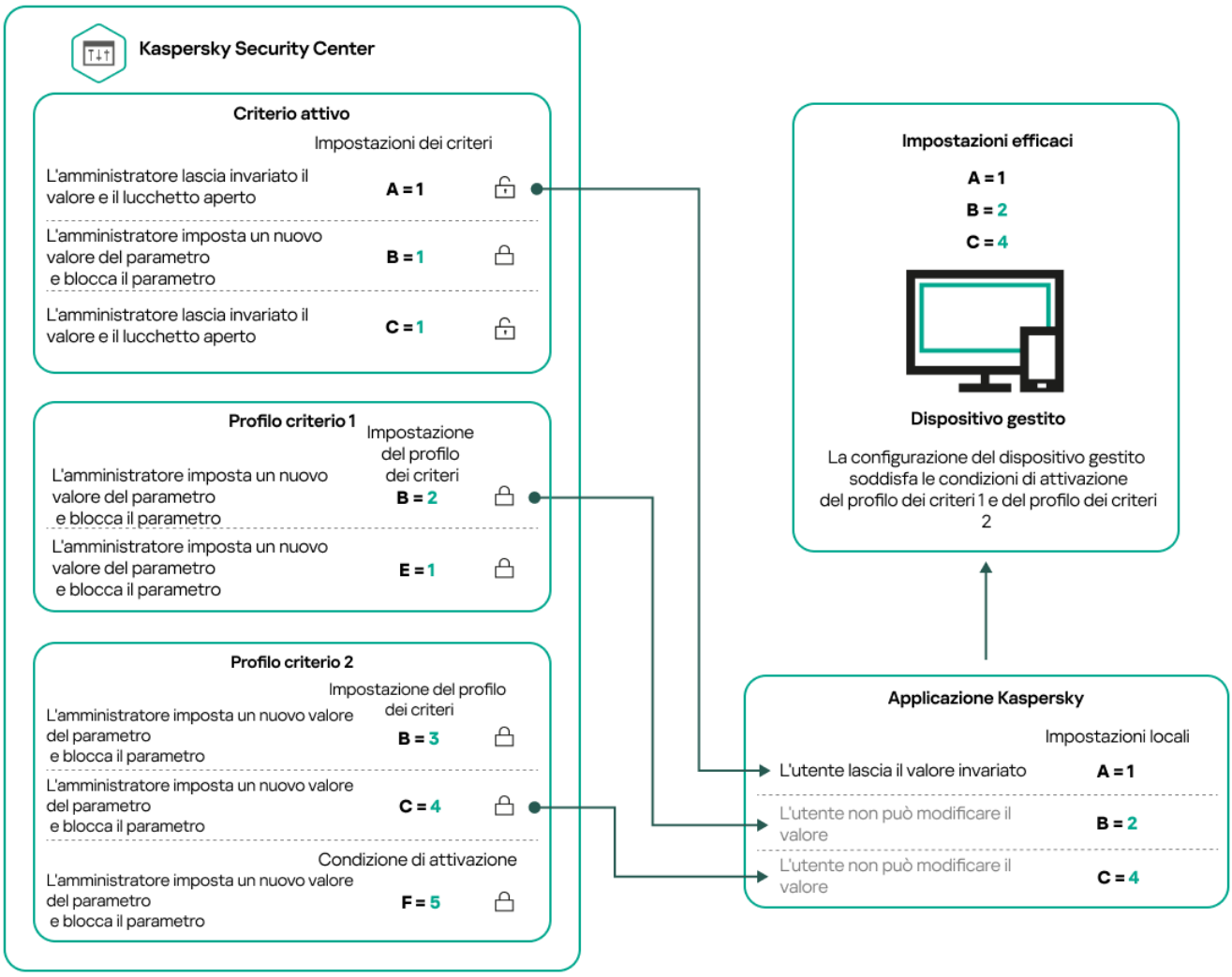
I profili criterio hanno le seguenti condizioni di assegnazione della priorità:

- La posizione di un profilo in un elenco di profili criterio indica la relativa priorità. È possibile modificare la priorità di un profilo criterio. La posizione più elevata in un elenco indica la massima priorità (vedere la figura seguente).



Definizione della priorità di un profilo criterio

- Le condizioni di attivazione dei profili criterio non dipendono l'una dall'altra. È possibile attivare più profili criterio contemporaneamente. Se più profili criterio influiscono sulla stessa impostazione, il dispositivo acquisisce il valore dell'impostazione dal profilo criterio con la priorità più elevata (vedere la figura seguente).



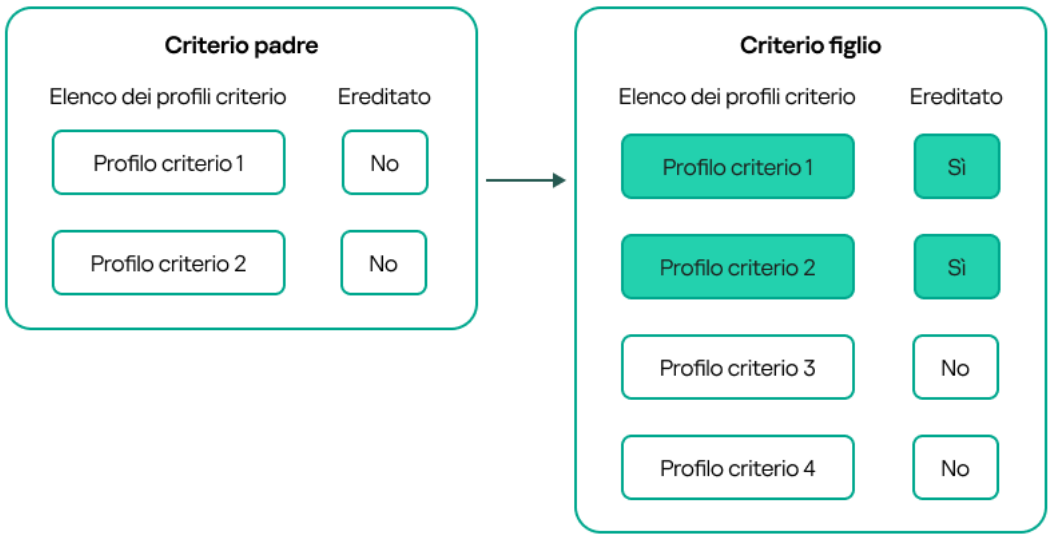
La configurazione del dispositivo gestito soddisfa le condizioni di attivazione di diversi profili criterio

Profili criterio in una gerarchia di ereditarietà

I profili criterio di diversi criteri di livello gerarchico soddisfano le seguenti condizioni:

- Un criterio di livello inferiore eredita i profili criterio da un criterio di livello superiore. Un profilo criterio ereditato da un criterio di livello superiore ottiene una priorità più elevata rispetto al livello del profilo criterio originale.

- Non è possibile modificare la priorità di un profilo criterio ereditato (vedere la figura seguente).



Ereditarietà dei profili criterio

Profili criterio con lo stesso nome

Se sono presenti due criteri con lo stesso nome in diversi livelli della gerarchia, questi criteri funzionano in base alle seguenti regole:

- Le impostazioni bloccate e la condizione di attivazione di un profilo criterio di livello superiore modificano le impostazioni e la condizione di attivazione di un profilo criterio di livello inferiore (vedere la figura seguente).

Il profilo figlio eredita i valori delle impostazioni da un profilo criterio principale

- Le impostazioni sbloccate e la condizione di attivazione di un profilo criterio di livello superiore non modificano le impostazioni e la condizione di attivazione di un profilo criterio di livello inferiore.

Modalità di implementazione delle impostazioni in un dispositivo gestito

L'implementazione di impostazioni ottimizzate in un dispositivo gestito può essere descritta come segue:

- I valori di tutte le impostazioni non bloccate vengono acquisiti dal criterio.
- Quindi vengono sovrascritti con i valori delle impostazioni dell'applicazione gestita.
- Vengono applicati i valori delle impostazioni bloccate del criterio ottimizzato. I valori delle impostazioni bloccate modificano i valori delle impostazioni ottimizzate sbloccate.

Gestione dei criteri

Questa sezione descrive i criteri di gestione e fornisce informazioni sulla visualizzazione dell'elenco dei criteri, sulla creazione di un criterio, sulla modifica di un criterio, sulla copia di un criterio, sullo spostamento di un criterio, sulla sincronizzazione forzata, sulla visualizzazione del grafico dello stato di distribuzione dei criteri e sull'eliminazione di un criterio.

Visualizzazione dell'elenco di criteri

È possibile visualizzare elenchi dei criteri creati per Administration Server o per qualsiasi gruppo di amministrazione.

Per visualizzare un elenco di criteri:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nella struttura dei gruppi di amministrazione selezionare il gruppo di amministrazione per cui si desidera visualizzare l'elenco di criteri.

   L'elenco di criteri viene visualizzato in formato di tabella. Se non sono presenti criteri, la tabella è vuota. È possibile mostrare o nascondere le colonne della tabella, modificarne l'ordine, visualizzare solo le righe che contengono un valore specificato o utilizzare la ricerca.

Creazione di un criterio

È possibile creare criteri, nonché modificare ed eliminare i criteri esistenti.

Per creare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare il gruppo di amministrazione per cui creare il criterio:
   - Per il gruppo radice.

     In questo caso, è possibile procedere al passaggio successivo.

- Per un sottogruppo:

  a. Fare clic sul collegamento del percorso corrente nella parte superiore della finestra.

  b. Nel pannello visualizzato, fare clic sul collegamento con il nome del sottogruppo desiderato.

  Il percorso corrente cambia per riflettere il sottogruppo selezionato.

3. Fare clic su **Aggiungi**.

   Verrà aperta la finestra **Selezionare l'applicazione**.

4. Selezionare l'applicazione per cui si desidera creare un criterio.

5. Fare clic su **Avanti**.

   Verrà visualizzata la finestra delle impostazioni del nuovo criterio, con la scheda **Generale** selezionata.

6. Se si desidera, modificare il nome predefinito, lo stato predefinito e le impostazioni di ereditarietà predefinite del criterio.

7. Selezionare la scheda **Impostazioni applicazione**.

   In alternativa, fare clic su **Salva** e uscire. Il criterio verrà visualizzato nell'elenco dei criteri e sarà possibile modificarne le impostazioni in un secondo momento.

8. Nella scheda **Impostazioni applicazione**, nel riquadro a sinistra selezionare la categoria desiderata e nel riquadro dei risultati a destra modificare le impostazioni del criterio. È possibile modificare le impostazioni del criterio in ciascuna categoria (sezione).

   Il set di impostazioni dipende dall'applicazione per cui si crea un criterio. Per i dettagli, fare riferimento ai seguenti elementi:

   - Configurazione di Administration Server
   - Impostazioni del criterio di Network Agent
   - Guida di Kaspersky Endpoint Security for Linux
   - Guida di Kaspersky Endpoint Security for Windows

   Per informazioni dettagliate sulle impostazioni delle altre applicazioni di protezione, fare riferimento alla documentazione relativa all'applicazione corrispondente.

   Quando si modificano le impostazioni, è possibile fare clic su **Annulla** per annullare l'ultima operazione.

9. Fare clic su **Salva** per salvare il criterio.

Il criterio verrà visualizzato nell'elenco dei criteri.

Impostazioni generali dei criteri

Generale

Nella scheda **Generale** è possibile modificare lo stato del criterio e specificare l'ereditarietà delle impostazioni criterio:

- Nella sezione **Stato criterio** è possibile selezionare una modalità criterio:
  - Attivo

    Se questa opzione è selezionata, il criterio diventa attivo.

    Per impostazione predefinita, questa opzione è selezionata.
  - Fuori sede

    Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.
  - Inattivo

    Se questa opzione è selezionata, il criterio diventa inattivo, ma viene comunque salvato nella cartella **Criteri**. Se necessario, il criterio può essere attivato.
- Nel gruppo di impostazioni **Ereditarietà impostazioni** è possibile configurare l'ereditarietà del criterio:
  - Eredita impostazioni dal criterio padre

    Se questa opzione è abilitata, i valori delle impostazioni del criterio vengono ereditati dal criterio di gruppo di livello superiore e pertanto vengono bloccati.

    Per impostazione predefinita, questa opzione è abilitata.
  - Forza ereditarietà impostazioni nei criteri figlio

    Se questa opzione è abilitata, una volta applicate le modifiche ai criteri, verranno eseguite le seguenti azioni:
    - I valori delle impostazioni dei criteri saranno propagati ai criteri dei sottogruppi di amministrazione, ovvero ai criteri secondari.
    - Nel gruppo **Ereditarietà impostazioni** della sezione **Generale** nella finestra delle proprietà di ogni criterio secondario, l'opzione **Eredita impostazioni dal criterio principale** sarà abilitata automaticamente.

    Se questa opzione è abilitata, le impostazioni dei criteri secondari vengono bloccate.

    Per impostazione predefinita, questa opzione è disabilitata.

Configurazione eventi

La scheda **Configurazione eventi** consente di configurare la registrazione degli eventi e le notifiche degli eventi. Gli eventi vengono distribuiti nelle seguenti schede in base al livello di importanza:

- **Critico**

  La sezione **Critico** non è visualizzata nelle proprietà del criterio di Network Agent.

- **Errore funzionale**
- **Avviso**
- **Informazioni**

In ogni sezione, l'elenco mostra i tipi di eventi e il periodo di archiviazione predefinito per gli eventi in Administration Server (in giorni). Facendo clic su un tipo di evento, è possibile specificare le seguenti impostazioni:

- **Registrazione eventi**

  È possibile specificare per quanti giorni archiviare l'evento e selezionare dove archiviarlo:

  - **Esporta nel sistema SIEM utilizzando Syslog**
  - **Archivia nel registro eventi del sistema operativo del dispositivo**
  - **Archivia nel registro eventi del sistema operativo in Administration Server**

- **Notifiche eventi**

  È possibile selezionare se si desidera essere informati dell'evento in uno dei seguenti modi:

  - **Notifica tramite e-mail**
  - **Notifica tramite SMS**
  - **Notifica tramite l'esecuzione di file eseguibile o script**
  - **Notifica tramite SNMP**

  Per impostazione predefinita, vengono utilizzate le impostazioni di notifica specificate nella scheda delle proprietà di Administration Server (ad esempio l'indirizzo del destinatario). Se si desidera, è possibile modificare queste impostazioni nelle schede **E-mail**, **SMS** e **File eseguibile da avviare**.

Cronologia revisioni

La scheda **Cronologia revisioni** consente di visualizzare l'elenco delle revisioni del criterio ed eseguire il rollback delle modifiche apportate al criterio, se necessario.

Modifica di un criterio

Per modificare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio che si desidera modificare.

   Verrà visualizzata la finestra delle impostazioni del criterio.
3. Specificare le impostazioni generali e le impostazioni dell'applicazione per cui si crea un criterio. Per i dettagli, fare riferimento ai seguenti elementi:

   - Configurazione di Administration Server

- Impostazioni del criterio di Network Agent
- Guida di Kaspersky Endpoint Security for Linux
- Guida di Kaspersky Endpoint Security for Windows

Per informazioni dettagliate sulle impostazioni delle altre applicazioni di protezione, fare riferimento alla documentazione relativa a tale applicazione.

4. Fare clic su **Salva**.

Le modifiche apportate al criterio saranno salvate nelle proprietà del criterio e verranno visualizzate nella sezione **Cronologia revisioni**.

Abilitazione e disabilitazione di un'opzione di ereditarietà dei criteri

Per abilitare o disabilitare l'opzione di ereditarietà in un criterio:

1. Aprire il criterio richiesto.
2. Aprire la scheda **Generale**.
3. Abilitare o disabilitare l'ereditarietà dei criteri:
   - Se si abilita **Eredita impostazioni dal criterio padre** in un criterio secondario e un amministratore blocca alcune impostazioni nel criterio principale, non è possibile modificare queste impostazioni nel criterio secondario.
   - Se si disabilita **Eredita impostazioni dal criterio padre** in un criterio secondario, è possibile modificare tutte le impostazioni nel criterio secondario, anche se alcune impostazioni sono bloccate nel criterio principale.
   - Se si abilita **Forza ereditarietà impostazioni nei criteri figlio** nel gruppo padre, viene abilitata l'opzione **Eredita impostazioni dal criterio padre** per tutti i criteri secondari. In questo caso, non è possibile disabilitare questa opzione per nessun criterio secondario. Tutte le impostazioni bloccate nel criterio principale vengono ereditate forzatamente nei gruppi figlio e non è possibile modificare queste impostazioni nei gruppi figlio.
4. Fare clic sul pulsante **Salva** per salvare le modifiche o fare clic sul pulsante **Annulla** per rifiutare le modifiche.

Per impostazione predefinita, l'opzione **Eredita impostazioni dal criterio padre** è abilitata per un nuovo criterio.

Se un criterio dispone di profili, tutti i criteri secondari ereditano tali profili.

Copia di un criterio

È possibile copiare i criteri da un gruppo di amministrazione a un altro.

Per copiare un criterio in un altro gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio (o ai criteri) che si desidera copiare.

3. Fare clic sul pulsante **Copia**.

   Sul lato destro dello schermo verrà visualizzata la struttura dei gruppi di amministrazione.

4. Nella struttura selezionare il gruppo di destinazione, ovvero il gruppo in cui si desidera copiare il criterio (o i criteri).

5. Fare clic sul pulsante **Copia** nella parte inferiore dello schermo.

6. Fare clic su **OK** per confermare l'operazione.

I criteri verranno copiati nel gruppo di destinazione con tutti i relativi profili. Lo stato di ciascun criterio copiato nel gruppo di destinazione sarà **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

Se un criterio con lo stesso nome del nuovo criterio spostato è già incluso nel gruppo di destinazione, al nome del nuovo criterio spostato viene aggiunto l'indice (<numero progressivo successivo>), ad esempio: (1).

Spostamento di un criterio

È possibile spostare i criteri da un gruppo di amministrazione a un altro. Ad esempio, si desidera eliminare un gruppo, ma utilizzare i relativi criteri per un altro gruppo. In questo caso, è possibile spostare il criterio dal gruppo precedente a quello nuovo prima di eliminare il gruppo precedente.

Per spostare un criterio in un altro gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

2. Selezionare la casella di controllo accanto al criterio (o ai criteri) che si desidera spostare.

3. Fare clic sul pulsante **Sposta**.

   Sul lato destro dello schermo verrà visualizzata la struttura dei gruppi di amministrazione.

4. Nella struttura selezionare il gruppo di destinazione, ovvero il gruppo in cui si desidera spostare il criterio (o i criteri).

5. Fare clic sul pulsante **Sposta** nella parte inferiore dello schermo.

6. Fare clic su **OK** per confermare l'operazione.

   Se un criterio non è ereditato dal gruppo di origine, verrà spostato nel gruppo di destinazione con tutti i relativi profili. Lo stato del criterio nel gruppo di destinazione è **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

   Se un criterio è ereditato dal gruppo di origine, rimane nel gruppo di origine. Viene copiato nel gruppo di destinazione con tutti i relativi profili. Lo stato del criterio nel gruppo di destinazione è **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

Se un criterio con lo stesso nome del nuovo criterio spostato è già incluso nel gruppo di destinazione, al nome del nuovo criterio spostato viene aggiunto l'indice (<numero progressivo successivo>), ad esempio: (1).

Esportazione di un criterio

Kaspersky Security Center Linux consente di salvare un criterio, le relative impostazioni e i profili dei criteri in un file KLP. È possibile utilizzare questo file KLP per importare il criterio salvato sia per Kaspersky Security Center Windows che per Kaspersky Security Center Linux.

Per esportare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio che si desidera esportare.

   Non è possibile esportare più criteri contemporaneamente. Se si selezionano più criteri, il pulsante **Esporta** verrà disabilitato.
3. Fare clic sul pulsante **Esporta**.
4. Nella finestra **Salva con nome** visualizzata, specificare il percorso e il nome del file di criteri. Fare clic sul pulsante **Salva**.

   La finestra **Salva con nome** viene visualizzata solo se si utilizza Google Chrome, Microsoft Edge oppure Opera. Se si utilizza un altro browser, il criterio di attività viene salvato automaticamente nella cartella **Download**.

Importazione di un criterio

Kaspersky Security Center Linux consente di importare un criterio da un file KLP. Il file KLP contiene il criterio esportato, le relative impostazioni e i profili dei criteri.

Per importare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul pulsante **Importa**.
3. Fare clic sul pulsante **Sfoglia** per scegliere un file di criteri da importare.
4. Nella finestra visualizzata, specificare il percorso del file di criteri KLP, quindi fare clic sul pulsante **Apri**. Si noti che è possibile selezionare solo un file di criteri.

   Viene avviata l'elaborazione del criterio.
5. Dopo che il criterio è stato elaborato correttamente, selezionare il gruppo di amministrazione a cui si desidera applicare il criterio.
6. Fare clic sul pulsante **Completa** per completare l'importazione del criterio.

Viene visualizzata la notifica con i risultati dell'importazione. Se il criterio viene importato correttamente, è possibile fare clic sul collegamento **Dettagli** per visualizzare le proprietà del criterio.

Dopo un'importazione riuscita, il criterio viene visualizzato nell'elenco dei criteri. Vengono importati anche le impostazioni e i profili del criterio. Indipendentemente dallo stato del criterio selezionato durante l'esportazione, il criterio importato è inattivo. È possibile modificare lo stato del criterio nelle proprietà del criterio.

Se il criterio appena importato ha un nome identico a quello di un criterio esistente, il nome del criterio importato viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Sincronizzazione forzata

Anche se Kaspersky Security Center Linux sincronizza automaticamente lo stato, le impostazioni, le attività e i criteri per i dispositivi gestiti, in alcuni casi l'amministratore ha l'esigenza di sapere esattamente se in un dato momento la sincronizzazione è già stata eseguita per un dispositivo specifico.

Sincronizzazione di un singolo dispositivo

Per forzare la sincronizzazione tra Administration Server e un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo che si desidera sincronizzare con Administration Server.

   Verrà visualizzata una finestra delle proprietà con la sezione **Generale** selezionata.
3. Fare clic sul pulsante **Forza sincronizzazione**.

L'applicazione sincronizzerà il dispositivo selezionato con Administration Server.

Sincronizzazione di più dispositivi

Per forzare la sincronizzazione tra Administration Server e più dispositivi gestiti:

1. Aprire l'elenco dei dispositivi di un gruppo di amministrazione o una selezione dispositivi:
   - Nel menu principale, passare a **Risorse (dispositivi)** → **Dispositivi gestiti**, fare clic sul collegamento del percorso nel campo **Percorso corrente** sopra l'elenco dei dispositivi gestiti, quindi selezionare il gruppo di amministrazione che contiene i dispositivi da sincronizzare.
   - Eseguire una selezione dei dispositivi per visualizzare l'elenco dei dispositivi.
2. Selezionare le caselle di controllo accanto ai dispositivi che si desidera sincronizzare con Administration Server.
3. Sopra l'elenco dei dispositivi gestiti, fare clic sul pulsante con i puntini di sospensione (...), quindi fare clic sul pulsante **Forza sincronizzazione**.

   L'applicazione sincronizzerà i dispositivi selezionati con Administration Server.
4. Nell'elenco dei dispositivi verificare che per i dispositivi selezionati l'ora dell'ultima connessione ad Administration Server sia cambiata all'ora corrente. Se l'ora non è cambiata, aggiornare il contenuto della pagina facendo clic sul pulsante **Aggiorna**.

I dispositivi selezionati vengono sincronizzati con Administration Server.

Visualizzazione dell'ora di invio di un criterio

Dopo aver modificato un criterio per un'applicazione Kaspersky sull'Administration Server, l'amministratore può verificare se il criterio modificato è stato distribuito a uno specifico dispositivo gestito. Un criterio può essere distribuito durante una sincronizzazione periodica o una sincronizzazione forzata.

Per visualizzare la data e l'ora in cui un criterio dell'applicazione è stato distribuito a un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo che si desidera sincronizzare con Administration Server.

   Verrà visualizzata una finestra delle proprietà con la sezione **Generale** selezionata.
3. Fare clic sulla scheda **Applicazioni**.
4. Selezionare l'applicazione per cui si desidera visualizzare la data di sincronizzazione del criterio.

   Verrà visualizzata la finestra del criterio dell'applicazione, con la sezione **Generale** selezionata e la data e l'ora di distribuzione del criterio visualizzate.

Visualizzazione del grafico dello stato di distribuzione dei criteri

In Kaspersky Security Center Linux è possibile visualizzare lo stato dell'applicazione dei criteri in ogni dispositivo in un grafico dello stato di distribuzione dei criteri.

Per visualizzare lo stato di distribuzione dei criteri in ogni dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al nome del criterio per cui si desidera visualizzare lo stato di distribuzione nei dispositivi.
3. Nel menu visualizzato selezionare il collegamento **Distribuzione**.

   Verrà visualizzata la finestra **Risultati della distribuzione di <Nome criterio>**.
4. Nella finestra **Risultati della distribuzione di <Nome criterio>** visualizzata viene visualizzata la **descrizione dello stato** del criterio.

È possibile modificare il numero di risultati visualizzati nell'elenco con la distribuzione dei criteri. Il numero massimo di dispositivi è 100.000.

Per modificare il numero dei dispositivi visualizzati nell'elenco con i risultati di distribuzione dei criteri:

1. Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Opzioni di interfaccia**.
2. In **Limite di dispositivi visualizzati nei risultati di distribuzione criteri**, immettere il numero di dispositivi (fino a 100.000).

   Il numero predefinito è 5000.
3. Fare clic su **Salva**.

   Le impostazioni verranno salvate e applicate.

Eliminazione di un criterio

È possibile eliminare un criterio se non è più necessario. Può essere eliminato solo un criterio che non viene ereditato nel gruppo di amministrazione specificato. Se un criterio viene ereditato, è possibile eliminarlo solo nel gruppo di livello superiore per cui è stato creato.

Per eliminare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio che si desidera eliminare e fare clic su **Elimina**.

   Il pulsante **Elimina** diventa non disponibile (visualizzato in grigio) se si seleziona un criterio ereditato.
3. Fare clic su **OK** per confermare l'operazione.

Il criterio verrà eliminato insieme a tutti i relativi profili.

Gestione dei profili criterio

Questa sezione illustra la gestione dei profili criterio e fornisce informazioni sulla visualizzazione dei profili di un criterio, sulla modifica della priorità di un profilo criterio, sulla creazione di un profilo criterio, sulla copia di un profilo criterio, sulla creazione di una regola di attivazione del profilo criterio e sull'eliminazione di un profilo criterio.

Visualizzazione dei profili di un criterio

Per visualizzare i profili di un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul nome del criterio di cui si desidera visualizzare i profili.

   Verrà visualizzata la finestra delle proprietà del criterio, con la scheda **Generale** selezionata.
3. Aprire la scheda **Profili criterio**.

L'elenco dei profili criterio viene visualizzato in formato di tabella. Se il criterio non dispone di profili, viene visualizzata una tabella vuota.

Modifica della priorità di un profilo criterio

Per modificare la priorità di un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.
2. Nella scheda **Profili criterio** selezionare la casella di controllo accanto al profilo criterio per cui si desidera modificare la priorità.

3. Impostare una nuova posizione del profilo criterio nell'elenco facendo clic su **Assegna priorità** o **Annulla priorità**.

   Più in alto è posizionato un profilo criterio nell'elenco, maggiore è la relativa priorità.

4. Fare clic sul pulsante **Salva**.

La priorità del profilo criterio selezionato verrà modificata e applicata.

Creazione di un profilo criterio

Per creare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio. Se il criterio non dispone di profili, viene visualizzata una tabella vuota.

2. Fare clic su **Aggiungi**.

3. Se si desidera, modificare il nome predefinito e le impostazioni di ereditarietà predefinite del profilo.

4. Selezionare la scheda **Impostazioni applicazione**.

   In alternativa, fare clic su **Salva** e uscire. Il profilo che è stato creato viene visualizzato nell'elenco dei profili criterio e sarà possibile modificarne le impostazioni in un secondo momento.

5. Nella scheda **Impostazioni applicazione**, nel riquadro a sinistra selezionare la categoria desiderata e nel riquadro dei risultati a destra modificare le impostazioni per il profilo. È possibile modificare le impostazioni del profilo criterio in ciascuna categoria (sezione).

   Quando si modificano le impostazioni, è possibile fare clic su **Annulla** per annullare l'ultima operazione.

6. Fare clic su **Salva** per salvare il profilo.

Il profilo verrà visualizzato nell'elenco dei profili criterio.

Copia di un profilo criterio

È possibile copiare un profilo criterio nel criterio corrente o in un altro, ad esempio se si desidera avere profili identici per criteri diversi. È anche possibile utilizzare la copia per disporre di due o più profili che differiscono solo per un numero limitato di impostazioni.

Per copiare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio. Se il criterio non dispone di profili, viene visualizzata una tabella vuota.

2. Nella scheda **Profili criterio** selezionare il profilo criterio che si desidera copiare.

3. Fare clic su **Copia**.

4. Nella finestra visualizzata selezionare il criterio in cui si desidera copiare il profilo.

   È possibile copiare un profilo criterio nello stesso criterio o in un criterio specificato.

5. Fare clic su **Copia**.

Il profilo criterio verrà copiato nel criterio selezionato. Il nuovo profilo copiato ha la priorità più bassa. Se si copia il profilo nello stesso criterio, al nome del nuovo profilo copiato viene aggiunto l'indice (), ad esempio: (1), (2).

Successivamente, è possibile modificare le impostazioni del profilo, inclusi il nome e la priorità. In questo caso, il profilo criterio originale non verrà modificato.

Creazione di una regola di attivazione del profilo criterio

Per creare una regola di attivazione per un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.

2. Nella scheda **Profili criterio** fare clic sul profilo criterio per cui è necessario creare una regola di attivazione.

   Se l'elenco dei profili criterio è vuoto, è possibile creare un profilo criterio.

3. Nella scheda **Regole di attivazione** fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra con le regole di attivazione del profilo criterio.

4. Specificare un nome per la regola.

5. Selezionare le caselle di controllo accanto alle condizioni che devono determinare l'attivazione del profilo criterio che si sta creando:

   - **Regole generali per l'attivazione del profilo criterio**

     Selezionare questa casella di controllo per configurare le regole di attivazione del profilo criterio nel dispositivo in base allo stato della modalità offline del dispositivo, alla regola per la connessione ad Administration Server e ai tag assegnati al dispositivo.

     Per questa opzione, specificare al passaggio successivo:

     - **Stato dispositivo**

       Definisce la condizione per la presenza del dispositivo nella rete:

       - **Online** - Il dispositivo è presente nella rete, pertanto Administration Server è disponibile.
       - **Offline** - Il dispositivo si trova in una rete esterna, pertanto Administration Server non è disponibile.
       - **N/D** - Il criterio non verrà applicato.

   - **La regola per la connessione ad Administration Server è attiva su questo dispositivo**

Scegliere la condizione di attivazione del profilo criterio (se la regola viene eseguita o meno) e selezionare il nome della regola.

La regola definisce il percorso di rete del dispositivo per la connessione ad Administration Server, le cui condizioni devono essere soddisfatte (o non devono essere soddisfatte) per l'attivazione del profilo criterio.

È possibile creare o configurare una descrizione del percorso di rete dei dispositivi per la connessione a un Administration Server in una regola per il passaggio di Network Agent.

- **Regole per il proprietario di un dispositivo specifico**

  Per questa opzione, specificare al passaggio successivo:

  - Proprietario dispositivo

    Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al proprietario. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

    - Il dispositivo appartiene al proprietario specificato (segno "=").
    - Il dispositivo non appartiene al proprietario specificato (segno "#").

      Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il proprietario dispositivo quando l'opzione è abilitata. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

  - Il proprietario dispositivo fa parte di un gruppo di protezione interno

    Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base all'appartenenza del proprietario a un gruppo di protezione interno di Kaspersky Security Center Linux. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

    - Il proprietario dispositivo è un membro del gruppo di protezione specificato (segno "=").
    - Il proprietario dispositivo non è un membro del gruppo di protezione specificato (segno "#").

      Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare un gruppo di protezione di Kaspersky Security Center Linux. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- Regole per le specifiche hardware

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base al volume della memoria e al numero di processori logici.

  Per questa opzione, specificare al passaggio successivo:

  - Dimensione RAM (MB)

Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al volume della RAM disponibile in tale dispositivo. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

- Le dimensioni della RAM del dispositivo sono inferiori al valore specificato (segno "<").
- Le dimensioni della RAM del dispositivo sono superiori al valore specificato (segno ">").

Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il volume della RAM nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Numero di processori logici**

  Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al numero di processori logici nel dispositivo. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

  - Il numero di processori logici nel dispositivo è inferiore o uguale al valore specificato (segno "<").
  - Il numero di processori logici nel dispositivo è superiore o uguale al valore specificato (segno ">").

  Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il numero di processori logici nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Regole per l'assegnazione dei ruoli**

  Per questa opzione, specificare al passaggio successivo:

  - **Attiva il profilo criterio in base allo specifico ruolo del proprietario del dispositivo**

    Selezionare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo a seconda del ruolo del proprietario. Aggiungere manualmente il ruolo dall'elenco dei ruoli esistenti.

    Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato.

- **Regole per l'utilizzo dei tag**

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base ai tag assegnati al dispositivo. È possibile attivare il profilo criterio nei dispositivi che dispongono o che non dispongono dei tag selezionati.

  Per questa opzione, specificare al passaggio successivo:

  - **Elenco di tag**

Nell'elenco di tag specificare una regola per l'inclusione dei dispositivi nel profilo criterio selezionando le caselle di controllo accanto ai tag appropriati.

È possibile aggiungere nuovi tag all'elenco immettendoli nel campo sopra l'elenco e facendo clic sul pulsante **Aggiungi**.

Il profilo criterio include i dispositivi con descrizioni che contengono tutti i tag selezionati. Se le caselle di controllo sono deselezionate, il criterio non viene applicato. Per impostazione predefinita, queste caselle di controllo sono deselezionate.

- Applica ai dispositivi senza i tag specificati

  Abilitare questa opzione se è necessario invertire la selezione di tag.

  Se questa opzione è abilitata, il profilo criterio include i dispositivi con descrizioni che non contengono alcuno dei tag selezionati. Se questa opzione è disabilitata, il criterio non viene applicato.

  Per impostazione predefinita, questa opzione è disabilitata.

- Regole per l'utilizzo di Active Directory

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base alla presenza del dispositivo in un'unità organizzativa di Active Directory o all'appartenenza del dispositivo (o del proprietario) a un gruppo di protezione di Active Directory.

  Per questa opzione, specificare al passaggio successivo:

  - Appartenenza del proprietario del dispositivo al gruppo di protezione di Active Directory

    Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo il cui proprietario appartiene al gruppo di protezione specificato. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

  - Appartenenza del dispositivo al gruppo di protezione di Active Directory

    Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

  - Allocazione del dispositivo nell'unità organizzativa di Active Directory

    Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo incluso nell'unità organizzativa di Active Directory specificata. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato.

    Per impostazione predefinita, questa opzione è disabilitata.

Il numero delle pagine aggiuntive della procedura guidata dipende dalle impostazioni selezionate nel primo passaggio. È possibile modificare le regole di attivazione del profilo criterio in un secondo momento.

6. Controllare l'elenco dei parametri configurati. Se l'elenco è corretto, fare clic su **Crea**.

Il profilo verrà salvato. Il profilo sarà attivato nel dispositivo quando vengono attivate le regole di attivazione.

Le regole di attivazione del profilo criterio create per il profilo sono visualizzate nelle proprietà del profilo criterio nella scheda **Regole di attivazione**. È possibile modificare o rimuovere qualsiasi regola di attivazione del profilo criterio.

È possibile attivare contemporaneamente più regole di attivazione.

Eliminazione di un profilo criterio

Per eliminare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.

2. Nella scheda **Profili criterio** selezionare la casella di controllo accanto al profilo criterio da eliminare e fare clic su **Elimina**.

3. Nella finestra visualizzata fare di nuovo clic su **Elimina**.

   Il profilo criterio viene eliminato. Se il criterio è ereditato da un gruppo di livello inferiore, il profilo rimane in tale gruppo, ma diventa il profilo criterio di tale gruppo. Questo avviene per eliminare un cambiamento significativo nelle impostazioni delle applicazioni gestite installate nei dispositivi dei gruppi di livello inferiore.

Impostazioni del criterio di Network Agent

Per configurare il criterio di Network Agent:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

2. Fare clic sul nome del criterio di Network Agent.

   Verrà visualizzata la finestra delle proprietà del criterio di Network Agent. La finestra delle proprietà contiene le schede e le impostazioni descritte di seguito.

Consultare la tabella di confronto che illustra nel dettaglio come si applicano le impostazioni riportate di seguito, a seconda del tipo di sistema operativo utilizzato.

Generale

In questa scheda, è possibile modificare il nome e lo stato del criterio e specificare l'ereditarietà delle impostazioni criterio:

- Nella sezione **Stato criterio** è possibile selezionare una delle seguenti modalità criterio:
  - **Criterio attivo**

Se questa opzione è selezionata, il criterio diventa attivo.

Per impostazione predefinita, questa opzione è selezionata.

- Criterio inattivo

  Se questa opzione è selezionata, il criterio diventa inattivo, ma viene comunque salvato nella cartella **Criteri**. Se necessario, il criterio può essere attivato.

- Nel gruppo di impostazioni **Ereditarietà impostazioni** è possibile configurare l'ereditarietà del criterio:

  - Eredita impostazioni dal criterio padre

    Se questa opzione è abilitata, i valori delle impostazioni del criterio vengono ereditati dal criterio di gruppo di livello superiore e pertanto vengono bloccati.

    Per impostazione predefinita, questa opzione è abilitata.

  - Forza ereditarietà impostazioni nei criteri figlio

    Se questa opzione è abilitata, una volta applicate le modifiche ai criteri, verranno eseguite le seguenti azioni:

    - I valori delle impostazioni dei criteri saranno propagati ai criteri dei sottogruppi di amministrazione, ovvero ai criteri secondari.
    - Nel gruppo **Ereditarietà impostazioni** della sezione **Generale** nella finestra delle proprietà di ogni criterio secondario, l'opzione **Eredita impostazioni dal criterio principale** sarà abilitata automaticamente.

    Se questa opzione è abilitata, le impostazioni dei criteri secondari vengono bloccate.

    Per impostazione predefinita, questa opzione è disabilitata.

Configurazione eventi

In questa scheda è possibile configurare la registrazione degli eventi e le notifiche degli eventi. Gli eventi sono distribuiti in base al livello di importanza nelle seguenti sezioni:

- **Errore funzionale**
- **Avviso**
- **Informazioni**

In ogni sezione, l'elenco mostra i tipi di eventi e il periodo di archiviazione predefinito per gli eventi in Administration Server (in giorni). Dopo aver fatto clic sul tipo di evento è possibile specificare le impostazioni di registrazione degli eventi e le notifiche sugli eventi selezionati nell'elenco. Per impostazione predefinita, le impostazioni di notifica comuni specificate per l'intero Administration Server vengono utilizzate per tutti i tipi di eventi. Tuttavia, è possibile modificare impostazioni specifiche per i tipi di eventi desiderati.

Ad esempio, nella sezione **Avviso**, è possibile configurare il tipo di evento **Si è verificato un problema di sicurezza**. Tali eventi possono ad esempio verificarsi quando lo spazio libero sul disco di un punto di distribuzione è inferiore a 2 GB (sono necessari almeno 4 GB per installare le applicazioni e scaricare gli aggiornamenti in remoto). Per configurare l'evento **Si è verificato un problema di sicurezza**, fare clic su di esso e specificare la posizione di archiviazione degli eventi che si sono verificati e le modalità di notifica.

Se Network Agent ha rilevato un problema di sicurezza, è possibile gestire tale problema utilizzando le impostazioni di un dispositivo gestito.

Impostazioni applicazione

Impostazioni

Nella sezione **Impostazioni** è possibile configurare il criterio di Network Agent:

- **Distribuisci i file solo tramite punti di distribuzione**

  Se questa opzione è abilitata, i Network Agent nei dispositivi gestiti recuperano gli aggiornamenti solo dai punti di distribuzione.

  Se questa opzione è disabilitata, i Network Agent nei dispositivi gestiti recuperano gli aggiornamenti dai punti di distribuzione o da Administration Server.

  Le applicazioni di protezione nei dispositivi gestiti recuperano gli aggiornamenti dalla sorgente impostata nell'attività di aggiornamento per ciascuna applicazione di protezione. Se si abilita l'opzione **Distribuisci i file solo tramite punti di distribuzione**, assicurarsi che Kaspersky Security Center Linux sia impostato come sorgente degli aggiornamenti nelle attività di aggiornamento.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima della coda di eventi (MB)**

  In questo campo è possibile specificare la quantità massima di spazio su disco che una coda di eventi può occupare.

  Il valore predefinito è 2 megabyte (MB).

- **L'applicazione può recuperare i dati estesi del criterio nel dispositivo**

Network Agent installato in un dispositivo gestito trasferisce le informazioni sul criterio dell'applicazione di protezione applicato all'applicazione di protezione (ad esempio Kaspersky Endpoint Security for Linux). È possibile visualizzare le informazioni trasferite nell'interfaccia dell'applicazione di protezione.

Network Agent trasferisce le seguenti informazioni:

- Ora della distribuzione del criterio al dispositivo gestito.
- Nome del criterio attivo al momento della distribuzione del criterio al dispositivo gestito.
- Nome del criterio fuori sede al momento della distribuzione del criterio al dispositivo gestito (non disponibile per Network Agent for Linux).
- Nome e percorso completo del gruppo di amministrazione che conteneva il dispositivo gestito al momento della distribuzione del criterio al dispositivo gestito.
- Elenco dei profili di criteri attivi con i relativi nomi e priorità al momento della distribuzione del criterio al dispositivo gestito.

È possibile utilizzare le informazioni per assicurarsi che venga applicato il criterio corretto al dispositivo e per la risoluzione dei problemi. Per impostazione predefinita, questa opzione è disabilitata.

- **Proteggi il servizio Network Agent dalle operazioni non autorizzate di rimozione o terminazione e impedisci la modifica delle impostazioni**

  Quando questa opzione è abilitata, dopo l'installazione di Network Agent in un dispositivo gestito, il componente non può essere rimosso o riconfigurato senza i privilegi richiesti. Il servizio Network Agent non può essere arrestato. Questa opzione non ha effetto sui controller di dominio.

  Abilitare questa opzione per proteggere Network Agent sulle workstation gestite con diritti di amministratore locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa password di disinstallazione**

  Se questa opzione è abilitata, facendo clic sul pulsante **Modifica** è possibile specificare la password per l'utilità klmover e la disinstallazione remota di Network Agent sui dispositivi basati su Windows.

  Per impostazione predefinita, questa opzione è disabilitata.

Archivi

Nella sezione **Archivi** è possibile selezionare i tipi di oggetti i cui dettagli verranno inviati da Network Agent ad Administration Server. Se la modifica di alcune impostazioni in questa sezione non è consentita dal criterio di Network Agent, non è possibile modificare tali impostazioni.

- **Informazioni dettagliate sulle applicazioni installate**

  Se questa opzione è abilitata, le informazioni sulle applicazioni installate nei dispositivi client vengono inviate ad Administration Server.

  Per impostazione predefinita, questa opzione è abilitata.

- Dettagli registro hardware

  Network Agent installato in un dispositivo invia informazioni sull'hardware del dispositivo ad Administration Server. È possibile visualizzare i dettagli hardware nelle proprietà del dispositivo.

  Assicurarsi che l'utilità lshw sia installata nei dispositivi Linux da cui si desidera recuperare i dettagli dell'hardware. I dettagli dell'hardware recuperati dalle macchine virtuali potrebbero essere incompleti a seconda dell'hypervisor utilizzato.

Connettività

La sezione **Connettività** include tre sottosezioni:

- **Rete**
- **Profili connessione**
- **Pianificazione connessione**

Nella sottosezione **Rete**, è possibile configurare la connessione ad Administration Server, abilitare l'utilizzo di una porta UDP e specificare il numero della porta UDP.

- Nel gruppo di impostazioni **Connetti ad Administration Server** è possibile configurare la connessione ad Administration Server e specificare l'intervallo di tempo per la sincronizzazione tra i dispositivi client e Administration Server:

  - Intervallo di sincronizzazione (min.)

    Network Agent sincronizza il dispositivo gestito con Administration Server. È consigliabile impostare l'intervallo di sincronizzazione (anche denominato heartbeat) su 15 minuti per 10.000 dispositivi gestiti.

    Se l'intervallo di sincronizzazione è impostato su meno di 15 minuti, la sincronizzazione viene eseguita ogni 15 minuti. Se l'intervallo di sincronizzazione è impostato su 15 minuti o più, la sincronizzazione viene eseguita all'intervallo di sincronizzazione specificato.

  - Comprimi traffico di rete

    Se questa opzione è abilitata, la velocità di trasferimento dei dati da parte di Network Agent viene aumentata attraverso una riduzione della quantità di informazioni da trasferire e una conseguente riduzione del carico di Administration Server.

    Il carico di lavoro sulla CPU del computer client potrebbe aumentare.

    Per impostazione predefinita, questa casella di controllo è abilitata.

  - Apri porte di Network Agent in Microsoft Windows Firewall

    Se questa opzione è abilitata, le porte, necessarie per l'utilizzo di Network Agent vengono aggiunte all'elenco di esclusioni di Microsoft Windows Firewall.

    Per impostazione predefinita, questa opzione è abilitata.

- Usa connessione SSL

  Se questa opzione è abilitata, la connessione ad Administration Server viene stabilita attraverso una porta sicura tramite SSL.

  Per impostazione predefinita, questa opzione è abilitata.

- Usa il gateway di connessione nel punto di distribuzione (se disponibile) con le impostazioni di connessione predefinite

  Se questa opzione è abilitata, viene utilizzato il gateway di connessione nel punto di distribuzione con le impostazioni specificate nelle proprietà del gruppo di amministrazione.

  Per impostazione predefinita, questa opzione è abilitata.

- Usa porta UDP

  Se è necessario che Network Agent si connetta ad Administration server attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in **Porta UDP**. Per impostazione predefinita, questa opzione è abilitata. La porta UDP predefinita per la connessione ad Administration Server è 15000.

- Numero di porta UDP

  In questo campo è possibile immettere il numero della porta UDP. Il numero di porta predefinito è 15000.

  Viene utilizzato il sistema decimale per i record.

Nella sottosezione **Profili connessione**, è possibile specificare le impostazioni del percorso di rete e abilitare la modalità fuori sede quando Administration Server non è disponibile:

- Impostazioni percorso di rete

  Le impostazioni del percorso di rete definiscono le caratteristiche della rete alla quale è connesso il dispositivo client e specificano le regole per il passaggio di Network Agent da un profilo di connessione Administration Server all'altro quando tali caratteristiche di rete subiscono variazioni.

- Profili connessione di Administration Server

  I profili di connessione sono supportati solo per i dispositivi che eseguono Windows.

  È possibile visualizzare e aggiungere profili per la connessione di Network Agent ad Administration Server. In questa sezione è inoltre possibile creare regole per il passaggio di Network Agent a diversi Administration Server quando si verificano i seguenti eventi:

  - Quando il dispositivo client si connette a un'altra rete locale
  - Quando il dispositivo perde la connessione con la rete locale dell'organizzazione
  - Quando cambia l'indirizzo del gateway di connessione o l'indirizzo del server DNS viene modificato

- Abilita la modalità fuori sede quando Administration Server non è disponibile

Se questa opzione è abilitata, in caso di utilizzo di questo profilo per la connessione, le applicazioni installate nel dispositivo client utilizzeranno i profili criterio per i dispositivi in modalità fuori sede, nonché i criteri fuori sede. Se non è definito alcun criterio fuori sede per l'applicazione, verrà utilizzato il criterio attivo.

Se questa opzione è disabilitata, le applicazioni utilizzeranno i criteri attivi.

Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Pianificazione connessione** è possibile specificare gli intervalli di tempo durante i quali Network Agent invia i dati ad Administration Server:

- **Connetti quando necessario**

  Se questa opzione è selezionata, la connessione viene stabilita quando Network Agent deve inviare i dati ad Administration Server.

  Per impostazione predefinita, questa opzione è selezionata.

- **Connetti negli intervalli di tempo specificati**

  Se questa opzione è selezionata, Network Agent si connette ad Administration Server all'ora specificata. È possibile aggiungere diversi periodi di tempo per la connessione.

Polling di rete per punti di distribuzione

Nella sezione **Polling di rete per punti di distribuzione** è possibile configurare il polling automatico della rete. È possibile utilizzare le seguenti opzioni per abilitare il polling e impostarne la frequenza:

- **Zeroconf**

  Se questa opzione è abilitata, il punto di distribuzione esegue automaticamente il polling della rete con i dispositivi IPv6 utilizzando le reti zero-configuration (definite anche *Zeroconf*). In questo caso, il polling dell'intervallo IP abilitati viene ignorato, poiché il punto di distribuzione esegue il polling dell'intera rete.

  Per iniziare a utilizzare Zeroconf è necessario soddisfare le seguenti condizioni:

  - Il punto di distribuzione deve eseguire Linux.
  - È necessario installare l'utilità avahi-browse nel punto di distribuzione.

  Se questa opzione è disabilitata, il punto di distribuzione non esegue il polling delle reti con i dispositivi IPv6.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Intervalli IP**

  Se l'opzione è abilitata, il punto di distribuzione esegue automaticamente il polling dell'intervallo IP in base alla pianificazione configurata facendo clic sul pulsante **Imposta pianificazione di polling**.

  Se questa opzione è disabilitata, il punto di distribuzione non esegue il polling degli intervalli IP.

  La frequenza di polling dell'intervallo IP per le versioni di Network Agent precedenti alla 10.2 può essere configurata nel campo **Intervallo di polling (min.)**. Il campo è disponibile se l'opzione è abilitata.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Controller di dominio**

Se l'opzione è abilitata, il punto di distribuzione esegue automaticamente il polling dei controller di dominio in base alla pianificazione configurata facendo clic sul pulsante **Imposta pianificazione di polling**.

Se questa opzione è disabilitata, il punto di distribuzione non esegue il polling dei controller di dominio.

La frequenza di polling dei controller di dominio per le versioni di Network Agent precedenti alla 10.2 può essere configurata nel campo **Intervallo di polling (min.)**. Il campo è disponibile se questa opzione è abilitata.

Per impostazione predefinita, questa opzione è disabilitata.

Impostazioni di rete per punti di distribuzione

Nella sezione **Impostazioni di rete per punti di distribuzione** è possibile specificare le impostazioni di accesso a Internet:

- **Usa server proxy**
- **Indirizzo**
- **Numero di porta**
- **Ignora il server proxy per gli indirizzi locali**

  Se questa opzione è abilitata, non viene utilizzato alcun server proxy per la connessione ai dispositivi nella rete locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Autenticazione server proxy**

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- **Nome utente**
- **Password**

Proxy KSN (punti di distribuzione)

Nella sezione **Proxy KSN (punti di distribuzione)** è possibile configurare l'applicazione per l'utilizzo del punto di distribuzione per l'inoltro delle richieste di Kaspersky Security Network (KSN) dai dispositivi gestiti:

- **Abilita proxy KSN da parte del punto di distribuzione**

Il servizio proxy KSN viene eseguito nel dispositivo utilizzato come punto di distribuzione. Utilizzare questa funzionalità per ridistribuire e ottimizzare il traffico nella rete.

Il punto di distribuzione invia le statistiche KSN, elencate nell'informativa di Kaspersky Security Network, a Kaspersky.

Per impostazione predefinita, questa opzione è disabilitata. L'attivazione di questa opzione ha effetto solo se le opzioni **Usa Administration Server come server proxy** e **Accetto di utilizzare Kaspersky Security Network** sono abilitate nella finestra delle proprietà di Administration Server.

È possibile assegnare il nodo di un cluster attivo-passivo a un punto di distribuzione e abilitare il proxy KSN in tale nodo.

- **Inoltra richieste KSN ad Administration Server**

  Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti ad Administration Server.

  Per impostazione predefinita, questa opzione è abilitata.

- **Accedi a KSN Cloud/KPSN direttamente tramite Internet**

  Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti a KSN Cloud o KPSN. Anche le richieste KSN generate nello stesso punto di distribuzione vengono inviate direttamente a KSN Cloud o KPSN.

- **Porta**

  Numero della porta TCP utilizzata dai dispositivi gestiti per la connessione al server proxy KSN. Il numero di porta predefinito è 13111.

- **Porta UDP**

  Se è necessario che Network Agent si connetta ad Administration server attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in **Porta UDP**. Per impostazione predefinita, questa opzione è abilitata. La porta UDP predefinita per la connessione ad Administration Server è 15000.

Aggiornamenti (punti di distribuzione)

Nella sezione **Aggiornamenti (punti di distribuzione)** è possibile abilitare la funzionalità per il download dei file diff, in modo che i punti di distribuzione acquisiscano gli aggiornamenti sotto forma di file diff dai server degli aggiornamenti Kaspersky.

Gestione riavvio

Nella sezione **Gestione riavvio** è possibile specificare l'azione che deve essere eseguita se il sistema operativo di un dispositivo gestito deve essere riavviato per utilizzare, installare o disinstallare correttamente un'applicazione:

- **Non riavviare il sistema operativo**

I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia automaticamente il sistema operativo se necessario**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Forza riavvio dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  - **Forza la chiusura delle applicazioni nelle sessioni bloccate**

    L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

    Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

    Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

    Per impostazione predefinita, questa opzione è disabilitata.

Utilizzo di Network Agent per Windows, Linux e macOS a confronto

L'utilizzo di Network Agent varia in base al sistema operativo del dispositivo. Anche le impostazioni del criterio e del pacchetto di installazione di Network Agent variano a seconda del sistema operativo. La tabella seguente mette a confronto le funzionalità di Network Agent e gli scenari di utilizzo disponibili per i sistemi operativi Windows, Linux e macOS.

Confronto fra le funzionalità di Network Agent

Funzionalità di Network Agent	Windows	Linux	macOS
Installazione			
Installazione tramite la clonazione di un'immagine del disco rigido dell'amministratore con il sistema operativo e Network Agent tramite strumenti di terzi	✓	✓	✓
Installazione con strumenti di terzi per l'installazione remota delle applicazioni	✓	✓	✓
Installazione manuale, eseguendo i programmi di installazione delle applicazioni nei dispositivi	✓	✓	✓
Installazione di Network Agent in modalità automatica	✓	✓	✓
Connessione manuale di un dispositivo client ad Administration Server. Utilità Klmover	✓	✓	✓
Installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center	✓	—	—
Distribuzione automatica di una chiave	✓	✓	✓
Sincronizzazione forzata	✓	✓	✓
Punto di distribuzione			
Utilizzo come punto di distribuzione	✓	✓	✓
Assegnazione automatica dei punti di distribuzione	✓	✓ Senza utilizzare Network Location Awareness (NLA).	✓ Senza utilizzare Network Location Awareness (NLA).
Modello offline per il download degli aggiornamenti	✓	✓	✓
Polling della rete	✓ • Polling intervallo IP • Polling del controller di dominio	✓ • Polling intervallo IP • Polling zeroconf • Polling del controller di dominio (Microsoft Active Directory, Samba 4 Active Directory)	—
Esecuzione del servizio proxy KSN da parte di un punto di	✓	✓	—

distribuzione			
Download degli aggiornamenti tramite i server degli aggiornamenti Kaspersky negli archivi dei punti di distribuzione che distribuiscono gli aggiornamenti ai dispositivi gestiti	✓	✓	— (Se uno o più dispositivi che eseguono Linux o macOS rientrano nell'ambito dell'attività Scarica aggiornamenti negli archivi dei punti di distribuzione, l'attività viene completata con lo stato Non riuscito, anche se è stata completata correttamente in tutti i dispositivi Windows.)
Installazione push delle applicazioni	✓	Limitata: non è possibile eseguire l'installazione push su dispositivi Linux utilizzando i punti di distribuzione macOS.	Limitata: non è possibile eseguire l'installazione push su dispositivi Windows utilizzando i punti di distribuzione macOS.
Utilizzo come server push	✓	✓	—
Gestione delle applicazioni di terzi			
Installazione remota delle applicazioni nei dispositivi	✓	✓	✓
Configurazione degli aggiornamenti del sistema operativo in un criterio di Network Agent	✓	—	—
Visualizzazione delle informazioni sulle vulnerabilità del software	✓	—	—
Scansione delle applicazioni per rilevare la presenza di vulnerabilità	✓	—	—
Aggiornamenti software	✓	—	—
Inventario del software installato nei dispositivi	✓	✓	—
Macchine virtuali			
Installazione di Network Agent in una macchina virtuale	✓	✓	✓
Ottimizzazione delle impostazioni per VDI (Virtual Desktop Infrastructure)	✓	✓	✓
Supporto delle macchine virtuali dinamiche	✓	✓	✓
Altro			
Azioni di controllo in un dispositivo client remoto utilizzando Condivisione desktop Windows	✓	—	—
Monitoraggio dello stato della protezione anti-virus	✓	✓	✓
Gestione dei riavvii dei dispositivi	✓	—	—
Supporto del rollback del file system	✓	✓	✓
Utilizzo di un Network Agent come gateway di connessione	✓	✓	✓
Gestione connessioni	✓	✓	✓
Passaggio di Network Agent da un Administration Server all'altro (automaticamente in base alla posizione di rete)	✓	—	✓
Verifica della connessione tra un dispositivo client e	✓	✓	✓

Administration Server. utilità klnagchk			
Connessione remota al desktop di un dispositivo client	✓	—	✓ Utilizzando il sistema VNC (Virtual Network Computing).
Download di un pacchetto di installazione indipendente tramite la Migrazione guidata	✓	✓	✓
Visualizzazione delle informazioni sull'hardware dei dispositivi client	✓	✓ Le informazioni sull'hardware dei dispositivi Linux inviate ad Administration Server da Network Agent installato in questi dispositivi sono limitate alle informazioni specificate nella descrizione delle impostazioni del dispositivo gestito.	—

Confronto tra le impostazioni di Network Agent in base ai sistemi operativi

La tabella seguente mostra quali impostazioni dei criteri di Network Agent sono disponibili a seconda del sistema operativo del dispositivo gestito in cui è stato installato Network Agent.

Impostazioni di Network Agent: confronto in base ai sistemi operativi

Sezione Impostazioni	Windows	Linux	macOS
Generale	✓	✓	✓
Configurazione eventi	✓	✓	✓
Impostazioni	✓	✓ Sono disponibili le seguenti opzioni: • **Distribuisci i file solo tramite punti di distribuzione** • **Dimensione massima della coda di eventi (MB)** • **L'applicazione può recuperare i dati estesi del criterio nel dispositivo**	✓
Archivi	✓	✓ Sono disponibili le seguenti opzioni: • **Informazioni dettagliate sulle applicazioni installate** • **Dettagli registro hardware**	—
Connettività → Rete	✓	✓ Ad eccezione dell'opzione **Apri porte di Network Agent in Microsoft Windows Firewall**.	✓
Connettività → Profili connessione	✓	—	✓
Connettività → Pianificazione connessione	✓	✓	✓
Polling di rete per punti di distribuzione	✓ Sono disponibili le seguenti opzioni: • **Rete Windows** • **Intervalli IP** • **Controller di dominio**	✓ Sono disponibili le seguenti opzioni: • **Zeroconf** • **Intervalli IP** • **Controller di dominio**	—
Impostazioni di rete per punti di distribuzione	✓	✓	✓

Proxy KSN (punti di distribuzione)	✓	✓	–
Aggiornamenti (punti di distribuzione)	✓	✓	–
Cronologia revisioni	✓	✓	✓

Configurazione manuale del criterio di Kaspersky Endpoint Security

Questa sezione offre suggerimenti per la configurazione del criterio di Kaspersky Endpoint Security. È possibile eseguire la configurazione nella finestra delle proprietà del criterio. Quando si modifica un'impostazione, fare clic sull'icona del lucchetto a destra del gruppo di impostazioni pertinente per applicare i valori specificati a una workstation.

Configurazione di Kaspersky Security Network

Kaspersky Security Network (KSN) è l'infrastruttura dei servizi cloud che contiene informazioni sulla reputazione di file, risorse Web e software. Kaspersky Security Network consente a Kaspersky Endpoint Security for Windows di rispondere più rapidamente a diversi tipi di minacce, migliora le prestazioni dei componenti della protezione e riduce la probabilità di falsi positivi. Per ulteriori informazioni su Kaspersky Security Network, vedere la Guida di Kaspersky Endpoint Security for Windows.

Per specificare le impostazioni consigliate di KSN:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio passare a **Impostazioni applicazione** → **Protezione minacce avanzata** → **Kaspersky Security Network**.
4. Verificare che l'opzione **Kaspersky Security Network** sia abilitata. L'utilizzo di questa opzione consente di ridistribuire e ottimizzare il traffico nella rete.

   > Se si utilizza Managed Detection and Response, è necessario abilitare l'opzione **Kaspersky Security Network** per il punto di distribuzione e abilitare la modalità KSN estesa.
5. Abilitare l'utilizzo dei server KSN se il servizio proxy KSN non è disponibile. I server KSN possono essere posizionati sul lato di Kaspersky (quando si utilizza KSN) o sul lato di terzi (quando si utilizza KPSN).
6. Fare clic su **OK**.

Sono state specificate le impostazioni consigliate di KSN.

Controllo dell'elenco delle reti protette dal Firewall

Verificare che il Firewall Kaspersky Endpoint Security for Windows protegga tutte le reti. Per impostazione predefinita il Firewall protegge le reti con i seguenti tipi di connessione:

- **Rete pubblica**. Le applicazioni di protezione, i firewall o i filtri non proteggono i dispositivi in una rete di questo tipo.
- **Rete locale**. L'accesso a file e stampanti è limitato per i dispositivi in questa rete.
- **Rete attendibile**. I dispositivi in tale rete sono protetti da attacchi e accessi non autorizzati a file e dati.

Se è stata configurata una rete personalizzata, assicurarsi che il Firewall la protegga. A tale scopo, controllare l'elenco delle reti nelle proprietà dei criteri di Kaspersky Endpoint Security for Windows. L'elenco potrebbe non contenere tutte le reti.

Per ulteriori informazioni sul Firewall vedere la Guida di Kaspersky Endpoint Security for Windows.

Per controllare l'elenco delle reti:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio passare a **Impostazioni applicazione** → **Protezione minacce essenziale** → **Firewall**.
4. In **Reti disponibili**, fare clic sul collegamento **Impostazioni di rete**.

   Verrà aperta la finestra **Connessioni di rete**. Questa finestra mostra l'elenco delle reti.
5. Se nell'elenco non è presente una rete, aggiungerla.

Disabilitazione della scansione delle unità di rete

Quando Kaspersky Endpoint Security for Windows esegue la scansione delle unità di rete, ciò può comportare un carico significativo su queste. È più pratico eseguire la scansione indiretta sui file server.

È possibile disabilitare la scansione delle unità di rete nelle proprietà dei criteri di Kaspersky Endpoint Security for Windows. Per una descrizione delle proprietà di questi criteri, consultare la Guida di Kaspersky Endpoint Security for Windows.

Per disabilitare la scansione delle unità di rete:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio, passare a **Impostazioni applicazione** → **Protezione minacce essenziale** → **Protezione minacce file**.
4. In **Ambito della protezione**, disabilitare l'opzione **Tutte le unità di rete**.
5. Fare clic su **OK**.

La scansione delle unità di rete è disabilitata.

Esclusione dei dettagli del software dalla memoria di Administration Server

È consigliabile evitare che Administration Server salvi le informazioni sui moduli software avviati nei dispositivi di rete. Di conseguenza, la memoria di Administration Server non viene sovraccaricata.

È possibile disabilitare il salvataggio di queste informazioni nelle proprietà dei criteri di Kaspersky Endpoint Security for Windows.

Per disabilitare il salvataggio delle informazioni sui moduli software installati:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio passare a **Impostazioni applicazione** → **Impostazioni generali** → **Rapporti e archivi**.
4. In **Trasferimento dei dati ad Administration Server** disabilitare la casella di controllo **Informazioni sulle applicazioni avviate** se è ancora abilitata nel criterio di primo livello.

   Quando questa casella di controllo è selezionata, il database di Administration Server salva informazioni su tutte le versioni di tutti i moduli software nei dispositivi connessi alla rete. Queste informazioni possono richiedere una quantità significativa di spazio su disco nel database di Kaspersky Security Center Linux (decine di gigabyte).

Le informazioni sui moduli software installati non vengono più salvate nel database di Administration Server.

Configurazione dell'accesso all'interfaccia di Kaspersky Endpoint Security for Windows nelle workstation

Se la protezione dalle minacce nella rete dell'organizzazione deve essere gestita in modalità centralizzata tramite Kaspersky Security Center Linux, specificare le impostazioni dell'interfaccia nelle proprietà del criterio di Kaspersky Endpoint Security for Windows, come descritto di seguito. In questo modo, si impedirà l'accesso non autorizzato a Kaspersky Endpoint Security for Windows sulle workstation e la modifica delle impostazioni di Kaspersky Endpoint Security for Windows.

Per una descrizione delle proprietà di questi criteri, consultare la Guida di Kaspersky Endpoint Security for Windows.

Per specificare le impostazioni dell'interfaccia consigliate:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio, passare a **Impostazioni applicazione** → **Impostazioni generali** → **Interfaccia**.

4. In **Interazione con l'utente**, selezionare l'opzione **Non visualizzare**. In questo modo, si disabilita la visualizzazione dell'interfaccia utente di Kaspersky Endpoint Security for Windows sulle workstation, quindi i relativi utenti non possono modificare le impostazioni di Kaspersky Endpoint Security for Windows.

5. In **Protezione tramite password**, abilitare l'interruttore. Questo riduce il rischio di modifiche non autorizzate o accidentali nelle impostazioni di Kaspersky Endpoint Security for Windows nelle workstation.

Sono state specificate le impostazioni consigliate per l'interfaccia di Kaspersky Endpoint Security for Windows.

Salvataggio degli eventi di criteri importanti nel database dell'Administration Server

Per evitare l'overflow del database di Administration Server, è consigliabile salvare solo gli eventi importanti nel database.

Per configurare la registrazione degli eventi importanti nel database di Administration Server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.

3. Nelle proprietà del criterio aprire la scheda **Configurazione eventi**.

4. Nella sezione **Critico** fare clic su **Aggiungi evento** e selezionare solo le caselle di controllo accanto ai seguenti eventi:

   - *Contratto di licenza con l'utente finale violato*
   - *L'esecuzione automatica dell'applicazione è disabilitata*
   - *Errore di attivazione*
   - *È stata rilevata una minaccia attiva. Si consiglia di avviare Disinfezione avanzata*
   - *Disinfezione non attuabile*
   - *Rilevato collegamento pericoloso aperto in precedenza*
   - *Processo terminato*
   - *Attività di rete bloccata*
   - *Attacco di rete rilevato*
   - *Avvio dell'applicazione non consentito*
   - *Accesso negato (database locali)*
   - *Accesso negato (KSN)*
   - *Errore di aggiornamento locale*

- *Impossibile avviare due attività contemporaneamente*
- *Errore durante l'interazione con Kaspersky Security Center*
- *Non tutti i componenti sono stati aggiornati*
- *Errore durante l'applicazione delle regole di criptaggio/decriptaggio dei file*
- *Errore durante l'abilitazione della modalità portatile*
- *Errore durante la disabilitazione della modalità portatile*
- *Impossibile caricare il modulo di criptaggio*
- *Il criterio non può essere applicato*
- *Errore durante la modifica dei componenti dell'applicazione*

5. Fare clic su **OK**.
6. Nella sezione **Errore funzionale**, fare clic su **Aggiungi evento** e selezionare solo la casella di controllo accanto all'evento *Impostazioni delle attività non valide. Impostazioni non applicate*.
7. Fare clic su **OK**.
8. Nella sezione **Avviso** fare clic su **Aggiungi evento** e selezionare solo le caselle di controllo accanto ai seguenti eventi:
   - *L'Auto-difesa è disabilitata*
   - *I componenti della protezione sono disabilitati*
   - *Chiave di riserva errata*
   - *È stato rilevato software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali (basi locali)*
   - *È stato rilevato software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali (KSN)*
   - *Oggetto eliminato*
   - *Oggetto disinfettato*
   - *L'utente ha scelto di non applicare il criterio di criptaggio*
   - *Il file è stato ripristinato dalla Quarantena nel server Kaspersky Anti Targeted Attack Platform dall'amministratore*
   - *Il file è stato messo in quarantena nel server di Kaspersky Anti Targeted Attack Platform dall'amministratore*
   - *Messaggio all'amministratore per il blocco dell'avvio di un'applicazione*
   - *Messaggio all'amministratore per il blocco dell'accesso a un dispositivo*
   - *Messaggio all'amministratore per il blocco dell'accesso a una pagina Web*

9. Fare clic su **OK**.

10. Nella sezione **Informazioni** fare clic su **Aggiungi evento** e selezionare solo le caselle di controllo accanto ai seguenti eventi:

    - *È stata creata una copia di backup dell'oggetto*
    - *Avvio dell'applicazione non consentito in modalità di test*

11. Fare clic su **OK**.

La registrazione degli eventi importanti nel database di Administration Server è configurata.

Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security

L'opzione di pianificazione ottimale e consigliata per Kaspersky Endpoint Security è **Quando vengono scaricati nuovi aggiornamenti nell'archivio** quando la casella di controllo **Usa automaticamente il ritardo casuale per l'avvio delle attività** è selezionata.

Finestra Kaspersky Security Network (KSN)

In questa sezione viene descritto come utilizzare un'infrastruttura di servizi online denominata Kaspersky Security Network (KSN). Vengono fornite informazioni dettagliate su KSN e istruzioni su come abilitare KSN, configurare l'accesso a KSN e visualizzare le statistiche di utilizzo del server proxy KSN.

Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Informazioni su KSN

Kaspersky Security Network (KSN) è un'infrastruttura di servizi online che consente di accedere alla Knowledge Base di Kaspersky, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliora l'efficacia di alcuni componenti della protezione e riduce il rischio di falsi positivi. KSN consente di utilizzare i database di reputazione di Kaspersky per recuperare informazioni sulle applicazioni installate nei dispositivi gestiti.

Partecipando a KSN, si autorizza l'invio automatico a Kaspersky di informazioni sul funzionamento delle applicazioni Kaspersky installate nei dispositivi client gestiti tramite Kaspersky Security Center Linux. Le informazioni vengono trasferite in base alle impostazioni di accesso a KSN correnti.

Kaspersky Security Center Linux supporta le seguenti soluzioni di infrastruttura KSN:

- *KSN Globale* è una soluzione che consente di scambiare informazioni con Kaspersky Security Network. Se si partecipa a KSN, si autorizza l'invio automatico a Kaspersky di informazioni sul funzionamento delle applicazioni Kaspersky installate nei dispositivi client gestiti tramite Kaspersky Security Center Linux. Le informazioni

vengono trasferite in base alle impostazioni di accesso a KSN correnti. Gli analisti di Kaspersky analizzano inoltre le informazioni ricevute e le includono nei database statistici e di reputazione di Kaspersky Security Network. Kaspersky Security Center Linux utilizza questa soluzione per impostazione predefinita.

- *Kaspersky Private Security Network (KPSN)* è una soluzione che consente agli utenti di dispositivi con applicazioni Kaspersky installate di ottenere l'accesso ai database di reputazione di Kaspersky Security Network e ad altri dati statistici, senza inviare dati a KSN Globale dai propri dispositivi. KPSN è progettato per i clienti aziendali che non sono in grado di partecipare al programma Kaspersky Security Network per uno dei seguenti motivi:

  - I dispositivi dell'utente non sono connessi a Internet.
  - La trasmissione dei dati all'esterno del paese o all'esterno della rete LAN aziendale è vietata dalla legge o limitata dai criteri di protezione aziendali.

  È possibile configurare le impostazioni di accesso di Kaspersky Private Security Network nella sezione **Impostazioni proxy KSN** della finestra delle proprietà di Administration Server.

All'utente verrà richiesto di partecipare a KSN durante l'esecuzione dell'Avvio rapido guidato. È possibile iniziare o smettere di utilizzare KSN in qualsiasi momento durante l'utilizzo dell'applicazione.

È necessario utilizzare KSN in conformità con l'Informativa KSN letta e accettata durante l'attivazione di KSN. Se l'Informativa KSN viene aggiornata, viene visualizzata quando si esegue l'upgrade di una versione di Administration Server. È possibile accettare o rifiutare l'Informativa KSN aggiornata. In caso di rifiuto, si continuerà a utilizzare KSN in conformità con la versione precedente dell'Informativa KSN già accettata.

Quando KSN è abilitato, Kaspersky Security Center Linux verifica se i server KSN sono accessibili per garantire il mantenimento del livello di protezione per i dispositivi gestiti. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici.

I dispositivi client gestiti da Administration Server interagiscono con KSN attraverso il server proxy KSN. Il server proxy KSN fornisce le seguenti funzionalità:

- I dispositivi client possono inviare richieste a KSN, ottenere informazioni da KSN e trasferire informazioni a KSN anche se non hanno accesso diretto a Internet.
- Il server proxy KSN memorizza nella cache i dati elaborati, riducendo in tal modo il carico sul canale in uscita e il tempo di attesa per ottenere le informazioni richieste da un dispositivo client.

È possibile configurare il server proxy KSN nella sezione **Impostazioni proxy KSN** della finestra delle proprietà di Administration Server.

Impostazione dell'accesso a KSN

È possibile configurare l'accesso a Kaspersky Security Network (KSN) in Administration Server e in un punto di distribuzione.

Per impostare l'accesso di Administration Server a KSN:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN**.

3. Spostare l'interruttore sulla posizione **Abilita proxy KSN in Administration Server Abilitato**.

   I dati vengono inviati dai dispositivi client a KSN in conformità con il criterio di Kaspersky Endpoint Security attivo in tali dispositivi client. Se questa casella di controllo è deselezionata, non verranno inviati dati a KSN da Administration Server e dai dispositivi client tramite Kaspersky Security Center Linux. I dispositivi client possono comunque inviare dati a KSN direttamente (ignorando Kaspersky Security Center Linux), in base alle relative impostazioni. Il criterio di Kaspersky Endpoint Security attivo nei dispositivi client determina quali dati saranno inviati a KSN direttamente (ignorando Kaspersky Security Center Linux) da tali dispositivi.

4. Impostare l'interruttore sulla posizione **Usa Kaspersky Security Network Abilitato**.

   Se questa opzione è abilitata, i dispositivi client invieranno i risultati dell'installazione delle patch a Kaspersky. Quando si abilita questa opzione, leggere e accettare le condizioni dell'informativa KSN.

   Se si utilizza KPSN, spostare l'interruttore sulla posizione **Usa Kaspersky Private Security Network Abilitato** e fare clic sul pulsante **Seleziona il file con le impostazioni del proxy KSN** per scaricare le impostazioni di KPSN (file con estensioni pkcs7 e pem). Una volta scaricate le impostazioni, l'interfaccia mostra il nome e i contatti del provider, nonché la data di creazione del file con le impostazioni di KPSN.

   Quando si sposta l'interruttore sulla posizione **Usa Kaspersky Private Security Network Abilitato**, viene visualizzato un messaggio con informazioni dettagliate su KPSN.

   Le seguenti applicazioni Kaspersky supportano KPSN:

   - Kaspersky Security Center Linux
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Endpoint Security for Windows

   Se si abilita KPSN in Kaspersky Security Center Linux, tali applicazioni ricevono informazioni sul supporto di KPSN Privato. Nella finestra delle impostazioni dell'applicazione, nella sottosezione **Kaspersky Security Network** della sezione **Protezione Minacce Avanzata**, vengono visualizzate le informazioni sul provider KSN selezionato: KSN o KPSN.

   > Kaspersky Security Center Linux non invia dati statistici a Kaspersky Security Network se KPSN è configurato nella sezione **Impostazioni proxy KSN** della finestra delle proprietà di Administration Server.

5. Se sono state configurate le impostazioni del server proxy nelle proprietà di Administration Server, ma l'architettura di rete richiede di utilizzare direttamente KPSN, abilitare l'opzione **Ignora impostazioni del server proxy durante la connessione a KPSN**. In caso contrario, le richieste dalle applicazioni gestite non possono raggiungere KPSN.

6. Configurare la connessione di Administration Server al servizio proxy KSN:

   - In **Impostazioni di connessione**, per **Porta TCP** specificare il numero della porta TCP che verrà utilizzata per la connessione al server proxy KSN. La porta predefinita per la connessione al server proxy KSN è la 13111.
   - Se si desidera che Administration Server si connetta al server proxy KSN attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** port e specificare il numero della porta in **Porta UDP**. Per impostazione predefinita, questa opzione è disabilitata e viene utilizzata la porta TCP. Se l'opzione è attivata, la porta UDP predefinita per la connessione al server KSN Proxy è 15111.
   - Se si desidera che Administration Server si connetta al server proxy KSN attraverso una porta HTTPS, abilitare l'opzione **Usa HTTPS** e specificare il numero della porta in **HTTPS tramite porta**. Per impostazione predefinita, questa opzione è disabilitata e viene utilizzata la porta TCP. Se l'opzione è attivata, la porta HTTPS predefinita per la connessione al server KSN Proxy è 17111.

7. Impostare l'interruttore sulla posizione **Connetti Administration Server secondari a KSN tramite Administration Server primario Abilitato**

   Se questa opzione è abilitata, gli Administration Server secondari utilizzano l'Administration Server primario come server proxy KSN. Se questa opzione è disabilitata, gli Administration Server secondari si connettono a KSN autonomamente. In questo caso, i dispositivi gestiti utilizzano gli Administration Server secondari come server proxy KSN.

   > Gli Administration Server secondari utilizzano l'Administration Server primario come server proxy se nel riquadro destro della sezione **Impostazioni proxy KSN** nelle proprietà degli Administration Server secondari l'interruttore è sulla posizione **Abilita proxy KSN in Administration Server Abilitato**.

8. Fare clic sul pulsante **Salva**.

Le impostazioni di accesso a KSN verranno salvate.

È inoltre possibile impostare l'accesso del punto di distribuzione a KSN, ad esempio se si desidera ridurre il carico sull'Administration Server. Il punto di distribuzione che opera come server proxy KSN invia richieste KSN direttamente dai dispositivi gestiti a Kaspersky, senza utilizzare l'Administration Server.

Per configurare l'accesso del punto di distribuzione a Kaspersky Security Network (KSN):

1. Accertarsi che il punto di distribuzione sia assegnato manualmente.
2. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.
3. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.
4. Fare clic sul nome del punto di distribuzione per aprire la relativa finestra delle proprietà.
5. Nella finestra delle proprietà del punto di distribuzione, nella sezione **Proxy KSN** abilitare l'opzione **Abilita proxy KSN da parte del punto di distribuzione**, quindi abilitare l'opzione **Accedi a KSN Cloud/KPSN direttamente tramite Internet**.
6. Fare clic su **OK**.

Il punto di distribuzione opererà come un server proxy KSN.

> Si noti che il punto di distribuzione non supporta l'autenticazione dei dispositivi gestiti tramite il protocollo NTLM.

Abilitazione e disabilitazione dell'utilizzo di KSN

Per abilitare l'utilizzo di KSN:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN**.

3. Spostare l'interruttore sulla posizione **Abilita proxy KSN in Administration Server Abilitato**.

Il server proxy KSN è abilitato e invia i dati a KSN per aumentare l'efficienza dei componenti di Kaspersky Security Center e migliorare le prestazioni delle applicazioni Kaspersky.

1. A seconda della soluzione di infrastruttura KSN in uso, abilitare gli interruttori corrispondenti.

   - Se si utilizza KSN Globale, spostare l'interruttore sulla posizione **Usa Kaspersky Security Network Abilitato**.

     L'invio dei dati a KSN è ora disponibile. Quando si abilita questa opzione, è necessario leggere e accettare le condizioni dell'Informativa KSN.

   - Se si utilizza KPSN, spostare l'interruttore sulla posizione **Usa Kaspersky Private Security Network Abilitato**, quindi fare clic sul pulsante **Seleziona il file con le impostazioni del proxy KSN** per scaricare le impostazioni di KPSN (file con estensioni pkcs7 e pem). Una volta scaricate le impostazioni, l'interfaccia mostra il nome e i contatti del provider, nonché la data di creazione del file con le impostazioni di KPSN.

     Quando si sposta l'interruttore sulla posizione **Usa Kaspersky Private Security Network Abilitato**, viene visualizzato un messaggio con informazioni dettagliate su KPSN.

2. Fare clic sul pulsante **Salva**.

Per disabilitare l'utilizzo di KSN:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN**.

3. Spostare l'interruttore sulla posizione **Abilita proxy KSN in Administration Server Disabilitato** per disabilitare il servizio proxy KSN.

4. Fare clic sul pulsante **Salva**.

Visualizzazione dell'Informativa KSN accettata

Quando si abilita Kaspersky Security Network (KSN), è necessario leggere e accettare l'Informativa KSN. È possibile visualizzare l'Informativa KSN accettata in qualsiasi momento.

Per visualizzare l'Informativa KSN accettata:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN**.

3. Fare clic sul collegamento **Visualizza l'Informativa di Kaspersky Security Network**.

Nella finestra visualizzata è possibile visualizzare il testo dell'Informativa KSN accettata.

Accettazione di un'Informativa KSN aggiornata

È necessario utilizzare KSN in conformità con l'Informativa KSN letta e accettata durante l'attivazione di KSN. Se l'Informativa KSN viene aggiornata, viene visualizzata quando si esegue l'upgrade di una versione di Administration Server. È possibile accettare o rifiutare l'Informativa KSN aggiornata. In caso di rifiuto, si continuerà a utilizzare KSN in conformità con la versione dell'Informativa KSN accettata precedentemente.

Dopo l'upgrade di una versione di Administration Server, l'Informativa KSN aggiornata viene visualizzata automaticamente. Se si rifiuta l'Informativa KSN aggiornata, è comunque possibile visualizzarla e accettarla in un secondo momento.

Per visualizzare e successivamente accettare o rifiutare un'Informativa KSN aggiornata:

1. Fare clic sul collegamento **Visualizza notifiche** nell'angolo superiore destro della finestra principale dell'applicazione.

   Verrà visualizzata la finestra **Notifiche**.

2. Fare clic sul collegamento **Visualizza l'Informativa KSN aggiornata**.

   Verrà visualizzata la finestra **Aggiornamento dell'Informativa di Kaspersky Security Network**.

3. Leggere l'Informativa KSN, quindi prendere una decisione facendo clic su uno dei seguenti pulsanti:

   - **Accetto l'Informativa KSN aggiornata**
   - **Usa KSN con l'Informativa precedente**

   A seconda della scelta, KSN continuerà a funzionare in conformità con i termini dell'Informativa KSN corrente o aggiornata. È possibile visualizzare il testo dell'Informativa KSN accettata nelle proprietà di Administration Server in qualsiasi momento.

Verifica per stabilire se il punto di distribuzione funziona come server proxy KSN

In un dispositivo gestito a cui è assegnato il ruolo di punto di distribuzione, è possibile abilitare il proxy di Kaspersky Security Network (KSN). Un dispositivo gestito funziona come server proxy KSN quando il servizio ksnproxy è in esecuzione nel dispositivo. È possibile controllare, attivare o disattivare questo servizio nel dispositivo in locale.

È possibile assegnare un dispositivo basato su Windows o Linux come punto di distribuzione. Il metodo di controllo del punto di distribuzione dipende dal sistema operativo di questo punto di distribuzione.

Per verificare se il punto di distribuzione basato su Linux funziona come server proxy KSN:

1. Nel dispositivo del punto di distribuzione, eseguire il comando `ps aux` per visualizzare l'elenco dei processi in esecuzione.

2. Nell'elenco dei processi in esecuzione, controllare se il processo `/opt/kaspersky/klnagent64/sbin/ksnproxy` è in esecuzione.

Se il processo `/opt/kaspersky/klnagent64/sbin/ksnproxy` è in esecuzione, Network Agent nel dispositivo partecipa a Kaspersky Security Network e funziona come server proxy KSN per i dispositivi gestiti inclusi nell'ambito del punto di distribuzione.

Per verificare se il punto di distribuzione basato su Windows funziona come server proxy KSN:

1. Nel dispositivo del punto di distribuzione, in Windows, aprire **Servizi** (**Tutti i programmi** → **Strumenti di amministrazione** → **Servizi**).

2. Nell'elenco dei servizi verificare se il servizio ksnproxy è in esecuzione.

   Se il servizio ksnproxy è in esecuzione, Network Agent nel dispositivo partecipa a Kaspersky Security Network e funziona come server proxy KSN per i dispositivi gestiti inclusi nell'ambito del punto di distribuzione.

Se si desidera, è possibile disattivare il servizio ksnproxy. In questo caso Network Agent nel punto di distribuzione interrompe la partecipazione a Kaspersky Security Network. Sono necessari i diritti di amministratore locale.

Gestione di attività

Questa sezione descrive le attività utilizzate da Kaspersky Security Center Linux.

Informazioni sulle attività

Kaspersky Security Center Linux consente di gestire le applicazioni di protezione Kaspersky installate nei dispositivi creando ed eseguendo *attività*. Le attività sono necessarie per l'installazione, l'avvio e l'arresto delle applicazioni, la scansione dei file, l'aggiornamento dei database e dei moduli software, oltre che per eseguire altre azioni sulle applicazioni.

Le attività per un'applicazione specifica possono essere create utilizzando Kaspersky Security Center Web Console solo se il plug-in di gestione per tale applicazione è installato in Kaspersky Security Center Web Console Server.

Le attività possono essere eseguite nell'Administration Server e nei dispositivi.

Le attività eseguite in Administration Server includono:

- Distribuzione automatica dei rapporti
- Download degli aggiornamenti nell'archivio
- Backup dei dati di Administration Server
- Manutenzione del database

I seguenti tipi di attività vengono eseguiti nei dispositivi:

- *Attività locali* - Attività eseguite in un dispositivo specifico

  Le attività locali possono essere modificate dall'amministratore utilizzando Kaspersky Security Center Web Console oppure dall'utente di un dispositivo remoto (ad esempio attraverso l'interfaccia dell'applicazione di protezione). Se un'attività locale viene modificata contemporaneamente dall'amministratore e dall'utente di un dispositivo gestito, hanno effetto le modifiche apportate dall'amministratore perché hanno una priorità più alta.

- *Attività di gruppo* - Attività eseguite su tutti i dispositivi di un gruppo specifico

A meno che non sia diversamente specificato nelle proprietà dell'attività, un'attività di gruppo si applica anche a tutti i sottogruppi del gruppo selezionato. Un'attività di gruppo influisce anche (facoltativamente) sui dispositivi connessi agli Administration Server secondari e virtuali distribuiti nel gruppo o in uno dei relativi sottogruppi.

- *Attività globali* - Attività eseguite su un set di dispositivi, indipendentemente dalla loro appartenenza a un gruppo.

Per ogni applicazione è possibile creare attività di gruppo, attività globali o attività locali.

È possibile apportare modifiche alle impostazioni delle attività, visualizzarne l'avanzamento, copiarle, esportarle, importarle ed eliminarle.

Le attività vengono avviate in un dispositivo solo se l'applicazione per cui l'attività è stata creata è in esecuzione.

I risultati dell'esecuzione delle attività vengono salvati nel registro eventi del sistema operativo in ciascun dispositivo, nel registro eventi del sistema operativo in Administration Server e nel database di Administration Server.

Non includere dati privati nelle impostazioni dell'attività. Ad esempio, non specificare la password dell'amministratore del dominio.

Informazioni sull'ambito dell'attività

L'*ambito di un'attività* è il set di dispositivi in cui viene eseguita l'attività. I tipi di ambito sono i seguenti:

- Per un'*attività locale*, l'ambito è il dispositivo stesso.
- Per un'*attività di Administration Server*, l'ambito è Administration Server.
- Per un'*attività di gruppo*, l'ambito è l'elenco dei dispositivi inclusi nel gruppo.

Durante la creazione di un'*attività globale*, è possibile utilizzare i seguenti metodi per specificare l'ambito:

- Specificare manualmente specifici dispositivi.

  È possibile utilizzare un indirizzo IP (o un intervallo IP) o un nome DNS come indirizzo del dispositivo.

- Importare un elenco di dispositivi da un file .txt con gli indirizzi dei dispositivi da aggiungere (ogni indirizzo deve essere specificato su una riga distinta).

  Se si importa un elenco di dispositivi da un file o se ne crea uno manualmente e i dispositivi vengono identificati con i rispettivi nomi, l'elenco deve contenere solo dispositivi per cui sono già state immesse le informazioni nel database di Administration Server. Inoltre, le informazioni devono essere state immesse al momento della connessione dei dispositivi o durante la device discovery.

- Specificare una selezione dispositivi.

  Nel corso del tempo, l'ambito un'attività si modifica, perché il set di dispositivi inclusi nella selezione cambia. Una selezione di dispositivi può essere creata sulla base degli attributi dei dispositivi, incluso il software installato in un dispositivo, e utilizzando i tag assegnati ai dispositivi. Una selezione dispositivi è il modo più flessibile per specificare l'ambito di un'attività.

Le attività per le selezioni dispositivi vengono sempre eseguite in base a una pianificazione da Administration Server. Queste attività non possono essere eseguite nei dispositivi che non dispongono di una connessione ad Administration Server. Le attività il cui ambito è specificato tramite altri metodi vengono eseguite direttamente nei dispositivi, pertanto non dipendono dalla connessione del dispositivo ad Administration Server.

Le attività per le selezioni dispositivi non vengono eseguite in base all'ora locale di un dispositivo, ma in base all'ora locale di Administration Server. Le attività il cui ambito è specificato tramite altri metodi vengono eseguite in base all'ora locale di un dispositivo.

Creazione di un'attività

Per creare un'attività:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni visualizzate.
3. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completa creazione attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
4. Fare clic sul pulsante **Fine**.

L'attività verrà creata e visualizzata nell'elenco delle attività.

Per creare una nuova attività assegnata ai dispositivi selezionati:

1. Nel menu principale accedere a **Risorse (dispositivi)** →**Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.
2. Nell'elenco dei dispositivi gestiti, selezionare le caselle di controllo accanto ai dispositivi per eseguire l'attività per gli stessi. È possibile utilizzare le funzioni di ricerca e filtraggio per trovare i dispositivi cercati.
3. Fare clic sul pulsante **Esegui attività**, quindi selezionare **Aggiungi nuova attività**.

   Verrà avviata la Creazione guidata nuova attività.

   Nel primo passaggio della procedura guidata, è possibile rimuovere i dispositivi selezionati da includere nell'ambito dell'attività. Seguire le istruzioni della procedura guidata.
4. Fare clic sul pulsante **Fine**.

L'attività viene creata per i dispositivi selezionati.

Avvio manuale di un'attività

L'applicazione avvia le attività in base alle impostazioni di pianificazione specificate nelle proprietà di ciascuna attività. È possibile avviare manualmente un'attività in qualsiasi momento dall'elenco di attività. In alternativa, è possibile selezionare i dispositivi nell'elenco **Dispositivi gestiti** e quindi avviare un'attività esistente per questi.

Per avviare un'attività manualmente:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Nell'elenco delle attività selezionare la casella di controllo accanto all'attività da avviare.
3. Fare clic sul pulsante **Avvia**.

L'attività viene avviata. È possibile controllare lo stato dell'attività nella colonna **Stato** o facendo clic sul pulsante **Risultato**.

Visualizzazione dell'elenco delle attività

È possibile visualizzare l'elenco delle attività create in Kaspersky Security Center Linux.

Per visualizzare l'elenco delle attività,

Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

Verrà visualizzato l'elenco delle attività. Le attività sono raggruppate in base ai nomi delle applicazioni a cui sono correlate. Ad esempio, l'attività *Installa l'applicazione in remoto* è correlata ad Administration Server e l'attività *Aggiornamento* fa riferimento a Kaspersky Endpoint Security.

Per visualizzare le proprietà di un'attività:

Fare clic sul nome dell'attività.

Verrà visualizzata la finestra delle proprietà dell'attività con diverse schede denominate. Ad esempio, **Tipo di attività** viene visualizzato nella scheda **Generale** e la pianificazione dell'attività nella scheda **Pianificazione**.

Impostazioni generali delle attività

Questa sezione contiene le impostazioni che è possibile configurare per la maggior parte delle attività. L'elenco delle impostazioni disponibili dipende dall'attività che si sta configurando.

Impostazioni specificate durante la creazione dell'attività

È possibile specificare le seguenti impostazioni durante la creazione di un'attività. Alcune di queste impostazioni possono anche essere modificate nelle proprietà dell'attività creata.

- Impostazioni per il riavvio del sistema operativo:
  - **Non riavviare il dispositivo**

I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

  L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

  Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

  Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

  Per impostazione predefinita, questa opzione è disabilitata.

- Impostazioni di pianificazione dell'attività:
  - **Impostazione Avvio pianificato:**
    - **Ogni N ore**

      L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

      Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

    - **Ogni N giorni**

      L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

      Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

    - **Ogni N settimane**

      L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

      Per impostazione predefinita, l'attività viene eseguita ogni venerdì all'ora di sistema corrente.

- **Ogni N minuti**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

  Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

- **Giornaliera (ora legale non supportata)**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

  Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center Linux.

  Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

- **Settimanale**

  L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Manualmente**

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è le 18:00.

- **Quando vengono scaricati nuovi aggiornamenti nell'archivio**

  L'attività viene eseguita dopo il download degli aggiornamenti nell'archivio. È ad esempio possibile utilizzare questa pianificazione per l'attività *Aggiornamento*.

- Al completamento di un'altra attività

  L'attività corrente viene avviata dopo il completamento di un'altra attività. È possibile selezionare la modalità di completamento dell'attività precedente (correttamente o con errori) per l'attivazione dell'avvio dell'attività corrente. Questo parametro funziona solo se entrambe le attività sono assegnate agli stessi dispositivi.

- Esegui attività non effettuate

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- Usa automaticamente il ritardo casuale per l'avvio delle attività

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

- Dispositivi a cui assegnare l'attività:

  - Selezionare i dispositivi della rete rilevati da Administration Server

    L'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.

    Questa opzione può ad esempio essere utilizzata in un'attività per l'installazione di Network Agent nei dispositivi non assegnati.

- Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco

  È possibile specificare nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

  Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

- Assegnare un'attività a una selezione dispositivi

  L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

- Assegnare un'attività a un gruppo di amministrazione

  L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

  Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

- Impostazioni per l'account:

  - Account predefinito

    L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

    Per impostazione predefinita, questa opzione è selezionata.

  - Specificare un account

    Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

  - Account

    Account tramite il quale viene eseguita l'attività.

  - Password

    Password dell'account con cui verrà eseguita l'attività.

Impostazioni specificate dopo la creazione dell'attività

È possibile specificare le seguenti impostazioni solo dopo la creazione di un'attività.

- Impostazioni delle attività di gruppo:
  - **Distribuisci ai sottogruppi**

    Questa opzione è disponibile solo nelle impostazioni delle attività di gruppo.

    Quando questa opzione è abilitata, l'ambito dell'attività include:

    - Il gruppo di amministrazione selezionato durante la creazione dell'attività.
    - I gruppi di amministrazione subordinati al gruppo di amministrazione selezionato a qualsiasi livello inferiore nella gerarchia dei gruppi.

    Quando questa opzione è disabilitata, l'ambito dell'attività include solo il gruppo di amministrazione selezionato durante la creazione dell'attività.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Distribuisci negli Administration Server secondari e virtuali**

    Quando questa opzione è abilitata, l'attività valida nell'Administration Server primario viene applicata anche negli Administration Server secondari (compresi quelli virtuali). Se un'attività dello stesso tipo esiste già nell'Administration Server secondario, nell'Administration Server secondario vengono applicate entrambe le attività: quella esistente e quella ereditata dall'Administration Server primario.

    Questa opzione è disponibile solo quando l'opzione **Distribuisci ai sottogruppi** è abilitata.

    Per impostazione predefinita, questa opzione è disabilitata.

- Impostazioni di pianificazione avanzate:
  - **Accendi i dispositivi utilizzando la funzione Wake-on-LAN prima di avviare l'attività (min)**

    Il sistema operativo nel dispositivo verrà avviato in base al periodo di tempo specificato prima dell'avvio dell'attività pianificata. Il periodo di tempo predefinito è cinque minuti.

    Abilitare questa opzione se si desidera eseguire l'attività in tutti i dispositivi client nell'ambito dell'attività, inclusi quelli che sono spenti al momento dell'avvio dell'attività.

    Se si desidera che il dispositivo si spenga automaticamente al termine dell'attività, abilitare l'opzione **Spegni i dispositivi dopo il completamento dell'attività**. Questa opzione è disponibile nella stessa finestra.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Spegni i dispositivi dopo il completamento dell'attività**

    Questa opzione può ad esempio essere abilitata per un'attività di aggiornamento dell'installazione che installa gli aggiornamenti nei dispositivi client ogni venerdì dopo l'orario lavorativo e quindi spegne tali dispositivi per il fine settimana.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Arresta se l'attività viene eseguita per più di (min)**

Al termine del periodo di tempo specificato, l'attività viene arrestata automaticamente, che sia stata completata o meno.

Abilitare questa opzione se si desidera interrompere (o arrestare) le attività che richiedono troppo tempo per l'esecuzione.

Per impostazione predefinita, questa opzione è disabilitata. Il tempo predefinito per l'esecuzione dell'attività è 120 minuti.

- Impostazioni di notifica:
  - Blocco **Salva cronologia attività**:
    - Archivia nel database di Administration Server per (giorni)

      Gli eventi dell'applicazione relativi all'esecuzione dell'attività in tutti i dispositivi client nell'ambito dell'attività vengono archiviati nell'Administration Server per il numero di giorni specificato. Al termine di questo periodo, le informazioni vengono eliminate da Administration Server.

      Per impostazione predefinita, questa opzione è abilitata.

    - Archivia nel registro eventi del sistema operativo del dispositivo

      Gli eventi dell'applicazione relativi all'esecuzione dell'attività vengono archiviati in locale nel registro eventi Syslog di ogni dispositivo client.

      Per impostazione predefinita, questa opzione è disabilitata.

    - Archivia nel registro eventi del sistema operativo in Administration Server

      Gli eventi dell'applicazione relativi all'esecuzione dell'attività in tutti i dispositivi client nell'ambito dell'attività vengono archiviati in modo centralizzato nel registro eventi Syslog del sistema operativo di Administration Server.

      Per impostazione predefinita, questa opzione è disabilitata.

    - Salva tutti gli eventi

      Se questa opzione è selezionata, nei registri eventi vengono salvati tutti gli eventi relativi all'attività.

    - Salva eventi correlati all'avanzamento dell'attività

      Se questa opzione è selezionata, nei registri eventi vengono salvati solo gli eventi relativi all'esecuzione dell'attività.

    - Salva solo i risultati dell'esecuzione dell'attività

      Se questa opzione è selezionata, nei registri eventi vengono salvati solo gli eventi relativi ai risultati dell'attività.

  - Notifica all'amministratore i risultati dell'esecuzione dell'attività

È possibile selezionare i metodi con cui inviare agli amministratori le notifiche relative ai risultati dell'esecuzione dell'attività: tramite e-mail, SMS o un file eseguibile. Per configurare la notifica, fare clic sul collegamento **Impostazioni**.

Per impostazione predefinita, tutti i metodi di notifica sono disabilitati.

- Notifica solo errori

  Se questa opzione è abilitata, agli amministratori viene inviata una notifica solo quando l'esecuzione di un'attività viene completata con un errore.

  Se questa opzione è disabilitata, agli amministratori viene inviata una notifica dopo il completamento dell'esecuzione di ogni attività.

  Per impostazione predefinita, questa opzione è abilitata.

- Impostazioni della protezione.
- Impostazioni dell'ambito dell'attività.

  A seconda del modo in cui viene determinato l'ambito dell'attività, sono disponibili le seguenti impostazioni:

  - Dispositivi

    Se l'ambito di un'attività è determinato in base a un gruppo di amministrazione, è possibile visualizzare tale gruppo. In questo caso, non è possibile apportare modifiche. Tuttavia, è possibile impostare l'opzione **Esclusioni dall'ambito dell'attività**.

    Se l'ambito di un'attività è determinato in base a un elenco di dispositivi, è possibile modificare l'elenco aggiungendo e rimuovendo dispositivi.

  - Selezione dispositivi

    È possibile modificare la selezione dispositivi a cui viene applicata l'attività.

  - Esclusioni dall'ambito dell'attività

    È possibile specificare gruppi di dispositivi a cui non deve essere applicata l'attività. I gruppi da escludere possono essere solo sottogruppi del gruppo di amministrazione a cui è applicata l'attività.

- **Cronologia revisioni**.

Esportazione di un'attività

Kaspersky Security Center Linux consente di salvare un'attività e le relative impostazioni in un file KLT. È possibile utilizzare questo file KLT per importare l'attività salvata sia per Kaspersky Security Center Windows che per Kaspersky Security Center Linux.

Per esportare un'attività:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.

2. Selezionare la casella di controllo accanto all'attività che si desidera esportare.

   Non è possibile esportare più attività contemporaneamente. Se si selezionano più attività, il pulsante **Esporta** verrà disabilitato. Neanche le attività di Administration Server sono disponibili per l'esportazione.

3. Fare clic sul pulsante **Esporta**.

4. Nella finestra **Salva con nome** visualizzata, specificare il percorso e il nome del file di attività. Fare clic sul pulsante **Salva**.

   La finestra **Salva con nome** viene visualizzata solo se si utilizza Google Chrome, Microsoft Edge oppure Opera. Se si utilizza un altro browser, il file di attività viene salvato automaticamente nella cartella **Download**.

Importazione di un'attività

Kaspersky Security Center Linux consente di importare un'attività da un file KLT. Il file KLT contiene l'attività esportata e le sue impostazioni.

Per importare un'attività:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

2. Fare clic sul pulsante **Importa**.

3. Fare clic sul pulsante **Sfoglia** per scegliere un file di attività da importare.

4. Nella finestra visualizzata, specificare il percorso del file di attività KLT, quindi fare clic sul pulsante **Apri**. Si noti che è possibile selezionare solo un file di attività.

   Viene avviata l'elaborazione dell'attività.

5. Dopo che l'attività è stata elaborata correttamente, selezionare i dispositivi a cui si desidera assegnare l'attività. A tale scopo, selezionare una delle seguenti opzioni:

   - Assegna attività a un gruppo di amministrazione

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

     Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

   - Specificare gli indirizzi dei dispositivi manualmente o importare gli indirizzi da un elenco

     È possibile specificare nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

     Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

   - Assegna attività a una selezione dispositivi

L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

6. Specificare l'ambito dell'attività.

7. Fare clic sul pulsante **Completa** per completare l'importazione dell'attività.

Viene visualizzata la notifica con i risultati dell'importazione. Se l'attività viene importata correttamente, è possibile fare clic sul collegamento **Dettagli** per visualizzare le proprietà dell'attività.

Dopo un'importazione riuscita, l'attività viene visualizzata nell'elenco delle attività. Vengono importate anche le impostazioni e la pianificazione dell'attività. L'attività verrà avviata in base alla sua pianificazione.

Se l'attività appena importata ha un nome identico a un'attività esistente, il nome dell'attività importata viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Avvio della Procedura guidata per la modifica della password delle attività

Per un'attività non locale, è possibile specificare un account con il quale deve essere eseguita l'attività. È possibile specificare l'account durante la creazione dell'attività o nelle proprietà di un'attività esistente. Se l'account specificato è utilizzato conformemente alle istruzioni di sicurezza dell'organizzazione, queste istruzioni possono occasionalmente richiedere la modifica della password dell'account. Quando scade la password dell'account e viene impostata una nuova password, l'attività non verrà avviata fino a quando non viene specificata la nuova password valida nelle proprietà dell'attività.

La Procedura guidata per la modifica della password delle attività consente di sostituire automaticamente la vecchia password con la nuova in tutte le attività in cui è specificato l'account. In alternativa, è possibile modificare manualmente questa password nelle proprietà di ogni attività.

Per avviare la Procedura guidata per la modifica della password delle attività:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

2. Fare clic su **Gestisci credenziali degli account per l'avvio delle attività**.

Seguire le istruzioni della procedura guidata.

Passaggio 1. Immissione delle credenziali

Specificare le nuove credenziali attualmente valide nel sistema. Quando si passa al passaggio successivo della procedura guidata, Kaspersky Security Center Linux verifica se il nome dell'account specificato corrisponde al nome dell'account nelle proprietà di ogni attività non locale. Se il nome dell'account corrisponde, la password nelle proprietà dell'attività verrà automaticamente sostituita con quella nuova.

Per specificare il nuovo account, selezionare un'opzione:

- Usa account corrente

  La procedura guidata utilizza il nome dell'account con cui si è attualmente connessi a Kaspersky Security Center Web Console. Specificare manualmente la password dell'account nel campo **Password corrente da utilizzare nelle attività**.

- Specifica un account diverso

  Specificare il nome dell'account con cui devono essere avviate le attività. Specificare la password dell'account nel campo **Password corrente da utilizzare nelle attività**.

Se si compila il campo **Password precedente (opzionale; se si desidera sostituirla con quella corrente)**, Kaspersky Security Center Linux sostituisce la password solo per le attività in cui si trovano sia il nome dell'account sia la password precedente. La sostituzione viene eseguita automaticamente. In tutti gli altri casi è necessario scegliere un'azione da eseguire nel passaggio successivo della procedura guidata.

Passaggio 2. Selezione di un'azione da eseguire

Se non è stata specificata la password precedente nel primo passaggio della procedura guidata o se la password precedente specificata non corrisponde alle password nelle proprietà delle attività, è necessario scegliere un'azione da eseguire per le attività rilevate.

Per scegliere un'azione per un'attività:

1. Selezionare la casella di controllo accanto all'attività per cui si desidera scegliere un'azione.
2. Eseguire una delle operazioni seguenti:
   - Per rimuovere la password nelle proprietà dell'attività, fare clic su **Elimina credenziali**.

     L'attività viene configurata per l'esecuzione con l'account predefinito.
   - Per sostituire la password con una nuova, fare clic su **Applica la modifica della password anche se la password precedente è errata o non specificata**.
   - Per annullare la modifica della password, fare clic su **Nessuna azione selezionata**.

Le azioni scelte vengono applicate una volta che si procede al passaggio successivo della procedura guidata.

Passaggio 3. Visualizzazione dei risultati

Nell'ultimo passaggio della procedura guidata, visualizzare i risultati per ciascuna attività rilevata. Per completare la procedura guidata, fare clic sul pulsante **Fine**.

Visualizzazione dei risultati dell'esecuzione delle attività memorizzati in Administration Server

Kaspersky Security Center Linux consente di visualizzare i risultati dell'esecuzione delle attività di gruppo, le attività per dispositivi specifici e le attività di Administration Server. Non possono essere visualizzati i risultati dell'esecuzione per le attività locali.

Per visualizzare i risultati di un'attività:

1. Nella finestra delle proprietà dell'attività selezionare la sezione **Generale**.
2. Fare clic sul collegamento **Risultati** per aprire la finestra **Risultati attività**.

Tag applicazione

Kaspersky Security Center Linux consente di contrassegnare le applicazioni dal registro delle applicazioni. Un tag è l'etichetta di un'applicazione che può essere utilizzata per raggruppare o cercare le applicazioni. Un tag assegnato alle applicazioni può essere utilizzato come condizione nelle selezioni dispositivi.

È ad esempio possibile creare il tag `[Browser]` e assegnarlo a tutti i browser, quali Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Creazione di un tag applicazione

Per creare un tag applicazione:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Tag applicazione**.
2. Fare clic su **Aggiungi**.
   Verrà visualizzata una finestra per il nuovo tag.
3. Immettere il nome del tag.
4. Fare clic su **OK** per salvare le modifiche.

Il nuovo tag verrà visualizzato nell'elenco dei tag applicazione.

Ridenominazione di un tag applicazione

Per rinominare un tag applicazione:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Tag applicazione**.
2. Selezionare la casella di controllo accanto al tag che si desidera rinominare, quindi fare clic su **Modifica**.
   Verrà visualizzata una finestra delle proprietà del tag.
3. Modificare il nome del tag.
4. Fare clic su **OK** per salvare le modifiche.

Il tag aggiornato verrà visualizzato nell'elenco dei tag applicazione.

Assegnazione di tag a un'applicazione

Per assegnare uno o più tag a un'applicazione:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Registro delle applicazioni**.
2. Fare clic sul nome dell'applicazione a cui si desidera assegnare i tag.
3. Fare clic sulla scheda **Tag**.

   La scheda mostra tutti i tag delle applicazioni presenti in Administration Server. Per i tag assegnati all'applicazione selezionata, la casella di controllo nella colonna **Tag assegnato** è selezionata.
4. Per i tag che si desidera assegnare, selezionare le caselle di controllo nella colonna **Tag assegnato**.
5. Fare clic su **Salva** per salvare le modifiche.

I tag verranno assegnati all'applicazione.

Rimozione dei tag assegnati a un'applicazione

Per rimuovere uno o più tag da un'applicazione:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Registro delle applicazioni**.
2. Fare clic sul nome dell'applicazione da cui si desidera rimuovere i tag.
3. Fare clic sulla scheda **Tag**.

   La scheda mostra tutti i tag delle applicazioni presenti in Administration Server. Per i tag assegnati all'applicazione selezionata, la casella di controllo nella colonna **Tag assegnato** è selezionata.
4. Per i tag che si desidera rimuovere, deselezionare le caselle di controllo nella colonna **Tag assegnato**.
5. Fare clic su **Salva** per salvare le modifiche.

I tag verranno rimossi dall'applicazione.

I tag dell'applicazione rimossi non vengono eliminati. Se si desidera, è possibile eliminarli manualmente.

Eliminazione di un tag applicazione

Per eliminare un tag applicazione:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Tag applicazione**.
2. Selezionare dall'elenco il tag applicazione da eliminare.
3. Fare clic sul pulsante **Elimina**.
4. Nella finestra visualizzata fare clic su **OK**.

Il tag applicazione verrà eliminato. Il tag eliminato viene rimosso automaticamente da tutte le applicazioni a cui è stato assegnato.

Concessione dell'accesso offline al dispositivo esterno bloccato da Controllo Dispositivi

Nel componente Controllo Dispositivi dei criteri di Kaspersky Endpoint Security, è possibile gestire l'accesso degli utenti ai dispositivi esterni installati nel dispositivo client o connessi a quest'ultimo (ad esempio, dischi rigidi, fotocamere o moduli Wi-Fi). Ciò consente di proteggere il dispositivo client dalle infezioni quando vengono collegati tali dispositivi esterni e impedire perdite o fughe di dati.

Se è necessario concedere l'accesso temporaneo al dispositivo esterno bloccato da Controllo Dispositivi ma il dispositivo esterno non può essere aggiunto all'elenco dei dispositivi attendibili, è possibile concedere l'accesso offline temporaneo al dispositivo esterno. Accesso offline significa che il dispositivo client non ha accesso alla rete.

È possibile concedere l'accesso offline al dispositivo esterno bloccato da Controllo dispositivi solo se l'opzione **Consenti richiesta di accesso temporaneo** è abilitata nelle impostazioni del criterio di Kaspersky Endpoint Security, nella sezione **Impostazioni applicazione** → **Controlli di sicurezza** → **Controllo dispositivi**.

La concessione dell'accesso offline al dispositivo esterno bloccato da Controllo Dispositivi comprende le seguenti fasi:

1. Nella finestra di dialogo Kaspersky Endpoint Security, l'utente del dispositivo che desidera avere accesso al dispositivo esterno bloccato genera un file della richiesta di accesso e lo invia all'amministratore di Kaspersky Security Center Linux.
2. Quando riceve questa richiesta, l'amministratore di Kaspersky Security Center Linux crea un file della chiave di accesso e lo invia all'utente del dispositivo.
3. Nella finestra di dialogo Kaspersky Endpoint Security l'utente del dispositivo attiva il file della chiave di accesso e ottiene l'accesso temporaneo al dispositivo esterno.

Per concedere l'accesso temporaneo al dispositivo esterno bloccato da Controllo Dispositivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.
2. In questo elenco, selezionare il dispositivo dell'utente che richiede l'accesso al dispositivo esterno bloccato da Controllo Dispositivi.

   È possibile selezionare un solo dispositivo.
3. Sopra l'elenco dei dispositivi gestiti, fare clic sul pulsante con i puntini di sospensione (...), quindi fare clic sul pulsante **Concedi l'accesso al dispositivo in modalità offline**.

4. Nella finestra **Impostazioni applicazione** visualizzata, nella sezione **Controllo Dispositivi**, fare clic sul pulsante **Sfoglia**.

5. Selezionare il file della richiesta di accesso ricevuto dall'utente, quindi fare clic sul pulsante **Apri**. Il file dovrebbe essere nel formato AKEY.

   Verranno visualizzati i dettagli del dispositivo bloccato a cui l'utente ha richiesto l'accesso.

6. Specificare il valore dell'impostazione **Durata accesso**.

   Questa impostazione definisce il periodo di tempo per cui verrà concesso all'utente l'accesso al dispositivo bloccato. Il valore predefinito è il valore specificato dall'utente durante la creazione del file della richiesta di accesso.

7. Specificare il periodo di tempo durante il quale la chiave di accesso può essere attivata sul dispositivo.

   Questa impostazione definisce il periodo di tempo per cui l'utente può attivare l'accesso al dispositivo bloccato utilizzando la chiave di accesso fornita.

8. Fare clic sul pulsante **Salva**.

9. Nella finestra visualizzata, selezionare la cartella di destinazione in cui salvare il file contenente la chiave di accesso per il dispositivo bloccato.

10. Fare clic sul pulsante **Salva**.

    Come risultato, quando si invia all'utente il file della chiave di accesso e l'utente lo attiva nella finestra di dialogo Kaspersky Endpoint Security, l'utente ha accesso temporaneo al dispositivo bloccato per il periodo specifico.

Utilizzo dell'utilità klscflag per aprire la porta 13291

È possibile automatizzare le operazioni di Kaspersky Security Center Linux tramite l'utilità klakaut. L'utilità klakaut e la relativa Guida sono disponibili nella cartella di installazione di Kaspersky Security Center Linux. Se si desidera utilizzare l'utilità klakaut, aprire la porta 13291 utilizzando l'utilità klscflag.

L'utilità klscflag modifica il valore del parametro KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Per aprire la porta 13291:

1. Eseguire il comando seguente nella riga di comando:
   ```
   $ /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. Riavviare il servizio Kaspersky Security Center Administration Server eseguendo il comando seguente:
   ```
   $ sudo systemctl restart kladminserver_srv
   ```

   La porta 13291 è aperta.

Per verificare se la porta 13291 è stata aperta correttamente:

Eseguire il comando seguente nella riga di comando:

```
$ /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\";"
```

Questo comando restituisce il seguente risultato:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)true
```

Il valore `true` indica che la porta è aperta. In caso contrario, viene visualizzato il valore `false`.

Registrazione dell'applicazione Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center Web Console

Per iniziare a utilizzare l'applicazione Kaspersky Industrial CyberSecurity for Networks tramite Kaspersky Security Center Web Console, è prima necessario registrarla in Kaspersky Security Center Web Console.

Per registrare l'applicazione Kaspersky Industrial CyberSecurity for Networks:

1. Assicurarsi di aver eseguito le seguenti operazioni:

   - Download e installazione del plug-in Web di Kaspersky Industrial CyberSecurity for Networks.

     È possibile eseguire questa operazione successivamente in attesa della sincronizzazione del server Kaspersky Industrial CyberSecurity for Networks con Administration Server. Dopo aver scaricato e installato il plug-in, la sezione **KICS for Networks** viene visualizzata nel menu principale di Kaspersky Security Center Web Console.

   - Nell'interfaccia Web di Kaspersky Industrial CyberSecurity for Networks, l'interazione con Kaspersky Security Center è configurata e abilitata. Per informazioni dettagliate, fare riferimento alla Guida in linea di Kaspersky Industrial CyberSecurity for Networks.

2. Spostare il dispositivo in cui è installato il server Kaspersky Industrial CyberSecurity for Networks dal gruppo Dispositivi non assegnati al gruppo Dispositivi gestiti:

   a. Nel menu principale accedere a, passare a **Individuazione e distribuzione** → **Dispositivi non assegnati**.

   b. Selezionare la casella di controllo accanto al dispositivo in cui è installato il server Kaspersky Industrial CyberSecurity for Networks.

   c. Fare clic sul pulsante **Sposta nel gruppo**.

   d. Nella gerarchia dei gruppi di amministrazione selezionare la casella di controllo accanto al gruppo **Dispositivi gestiti**.

   e. Fare clic sul pulsante **Sposta**.

3. Aprire la finestra delle proprietà del dispositivo in cui è installato il server Kaspersky Industrial CyberSecurity for Networks.

4. Nella pagina delle proprietà del dispositivo, nella sezione **Generale**, selezionare l'opzione **Non eseguire la disconnessione da Administration Server**, quindi fare clic sul pulsante **Salva**.

5. Nella pagina delle proprietà del dispositivo selezionare la sezione **Applicazioni**.

6. Nella sezione **Applicazioni**, selezionare Kaspersky Security Center Network Agent.

7. Se lo stato corrente dell'applicazione è *Arrestata*, attendere finché non diventa *In esecuzione*.

   L'operazione può richiedere fino a 15 minuti. Se non è ancora stato installato il plug-in Web di Kaspersky Industrial CyberSecurity for Networks, è possibile farlo.

8. Se si desidera visualizzare le statistiche di Kaspersky Industrial CyberSecurity for Networks, è possibile aggiungere widget nella dashboard. Per aggiungere i widget, procedere come segue:

   a. Nel menu principale, passare a **Monitoraggio e segnalazione** → **Dashboard**.

   b. Nella dashboard, fare clic sul pulsante **Aggiungi o ripristina widget web**.

   c. Nel menu del widget visualizzato selezionare **Altro**.

   d. Selezionare i widget da aggiungere:

      - Mappa di distribuzione di KICS for Networks
      - Informazioni sui server di KICS for Networks
      - Eventi aggiornati di KICS for Networks
      - Dispositivi con problemi in KICS for Networks
      - Eventi critici in KICS for Networks
      - Stati in KICS for Networks

9. Per passare all'interfaccia web di Kaspersky Industrial CyberSecurity for Networks, procedere come segue:

   a. Nel menu principale, passare a **KICS for Networks** → **Cerca**.

   b. Fare clic sul pulsante **Trova eventi o dispositivi**.

   c. Nella finestra **Parametri query** visualizzata, fare clic sul campo **Server**.

   d. Selezionare Kaspersky Industrial CyberSecurity for Networks Server nell'elenco a discesa dei server integrati con Kaspersky Security Center, quindi fare clic sul pulsante **Trova**.

   e. Fare clic sul collegamento **Vai al server** accanto al nome del server Kaspersky Industrial CyberSecurity for Networks.

      Viene visualizzata la pagina di accesso di Kaspersky Industrial CyberSecurity for Networks.

      Per accedere all'interfaccia Web di Kaspersky Industrial CyberSecurity for Networks, è necessario fornire le credenziali dell'account utente dell'applicazione.

Gestione di utenti e ruoli utente

Questa sezione descrive gli utenti e i ruoli utente e fornisce istruzioni per la creazione e la modifica di questi elementi, per l'assegnazione di ruoli e gruppi agli utenti e per l'associazione dei profili criterio ai ruoli.

Informazioni sugli account utente

Kaspersky Security Center Linux consente di gestire account utente e gruppi di protezione. L'applicazione supporta tre tipi di account:

- Account dei dipendenti dell'organizzazione. Administration Server recupera i dati degli account degli utenti di dominio durante il polling del controller del dominio dell'organizzazione.
- Account degli utenti locali. Account locali dei dispositivi gestiti, nonché account locali del dispositivo in cui è installato Administration Server.
- Account di utenti interni di Kaspersky Security Center Linux. È possibile creare account di utenti interni. Questi account vengono utilizzati solo all'interno di Kaspersky Security Center Linux.

Non è possibile utilizzare il gruppo kladmins per accedere a Kaspersky Security Center Web Console in Kaspersky Security Center Linux. Il gruppo kladmins può contenere solo gli account utilizzati per avviare i servizi di Kaspersky Security Center Linux.

Per visualizzare le tabelle degli account utente e dei gruppi di protezione:

1. Nel menu principale accedere a **Utenti e ruoli** → **Utenti e gruppi**.
2. Selezionare la scheda **Utenti** o **Gruppi**.

Si apre la tabella degli utenti o dei gruppi di protezione. Se si desidera visualizzare la tabella solo con utenti o gruppi interni o solo con utenti o gruppi locali, impostare i criteri di filtro **Sottotipo** rispettivamente su **Interno** o **Locale**.

Informazioni sui ruoli utente

Un *ruolo utente* (anche denominato *ruolo*) è un oggetto contenente un set di diritti e privilegi. Un ruolo può essere associato alle impostazioni delle applicazioni Kaspersky installate in un dispositivo utente. È possibile assegnare un ruolo a un set di utenti o a un set di gruppi di protezione a qualsiasi livello nella gerarchia dei gruppi di amministrazione, di Administration Server o a livello di oggetti specifici.

Se i dispositivi vengono gestiti tramite una gerarchia di Administration Server che include Administration Server virtuali, si noti che è possibile creare, modificare o eliminare i ruoli utente solo da un Administration Server fisico. È quindi possibile propagare i ruoli utente agli Administration Server secondari, inclusi quelli virtuali.

È possibile associare i ruoli utente ai profili criterio. Se a un utente viene assegnato un ruolo, tale utente ottiene le impostazioni di protezione necessarie per eseguire le funzioni lavorative.

Un ruolo utente può essere associato agli utenti dei dispositivi in un gruppo di amministrazione specifico.

Ambito del ruolo utente

Un *ambito di un ruolo utente* è una combinazione di utenti e gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Vantaggi dell'utilizzo dei ruoli

Un vantaggio dell'utilizzo dei ruoli è che non è necessario specificare le impostazioni di protezione per ciascuno dei dispositivi gestiti o per ciascuno degli utenti separatamente. Il numero di utenti e dispositivi in un'azienda può essere piuttosto elevato, ma il numero delle diverse funzioni lavorative che richiedono differenti impostazioni di protezione è notevolmente inferiore.

Differenze rispetto all'utilizzo dei profili criterio

I profili criterio sono le proprietà di un criterio creato per ciascuna applicazione Kaspersky separatamente. Un ruolo è associato a molti profili criterio creati per diverse applicazioni. Pertanto, un ruolo è un metodo per riunire le impostazioni per un determinato tipo di utente in un'unica posizione.

Configurazione dei diritti di accesso alle funzionalità dell'applicazione. Controllo dell'accesso basato sui ruoli

Kaspersky Security Center Linux offre l'accesso in base al ruolo alle funzionalità di Kaspersky Security Center Linux e delle applicazioni Kaspersky gestite.

È possibile configurare i diritti di accesso alle funzionalità dell'applicazione per gli utenti di Kaspersky Security Center Linux in uno dei seguenti modi:

- Attraverso la configurazione dei diritti per ciascun utente o gruppo di utenti singolarmente.
- Attraverso la creazione di ruoli utente standard con un set di diritti predefinito e l'assegnazione di tali ruoli agli utenti sulla base dell'ambito delle relative mansioni lavorative.

L'applicazione dei ruoli utente ha lo scopo di semplificare e abbreviare le procedure di routine per la configurazione dei diritti di accesso degli utenti alle funzionalità dell'applicazione. I diritti di accesso all'interno di un ruolo vengono configurati in base alle attività standard e all'ambito delle mansioni lavorative degli utenti.

Ai ruoli utente possono essere assegnati nomi corrispondenti ai rispettivi scopi. È possibile creare un numero illimitato di ruoli nell'applicazione.

È possibile utilizzare i ruoli utente predefiniti con un set di diritti già configurato oppure creare nuovi ruoli e configurare autonomamente i diritti richiesti.

Diritti di accesso alle funzionalità dell'applicazione

La tabella seguente mostra le funzionalità di Kaspersky Security Center Linux con i diritti di accesso per gestire le attività, i rapporti e le impostazioni associati e per eseguire le azioni utente associate.

Per eseguire le azioni utente elencate nella tabella, un utente deve disporre del diritto specificato accanto all'azione.

I diritti **Lettura**, **Scrittura** ed **Esecuzione** sono applicabili a qualsiasi attività, rapporto o impostazione. Oltre a questi diritti, un utente deve disporre del diritto **Esegui operazioni per le selezioni di dispositivi** per gestire attività, rapporti o impostazioni relativi alle selezioni dispositivi.

L'area funzionale **Caratteristiche generali**: **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** è destinata a scopi di controllo. Quando gli utenti ottengono i diritti di **Lettura** in quest'area funzionale, ottengono l'accesso completo in **Lettura** a tutti gli oggetti e sono in grado di eseguire qualsiasi attività creata su selezioni di dispositivi connessi ad Administration Server tramite Network Agent con diritti di amministratore locale (root per Linux). Si consiglia di concedere con attenzione questi diritti a un gruppo limitato di utenti che ne hanno bisogno per svolgere le proprie funzioni ufficiali.

Tutte le attività, i rapporti, le impostazioni e i pacchetti di installazione mancanti nella tabella appartengono all'area funzionale **Caratteristiche generali: Funzionalità di base**.

Diritti di accesso alle funzionalità dell'applicazione

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: **Gestione dei gruppi di amministrazione**	**Scrittura**	• Aggiungere un dispositivo a un gruppo di amministrazione: **Scrittura** • Eliminare un dispositivo da un gruppo di amministrazione: **Scrittura** • Aggiungere un gruppo di amministrazione a un altro gruppo di amministrazione: **Scrittura** • Eliminare un gruppo di amministrazione da un altro gruppo di amministrazione: **Scrittura**	None	None	None
Caratteristiche generali: **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi**	**Lettura**	Ottenere l'accesso in lettura a tutti gli oggetti: **Lettura**	None	None	L'accesso viene concesso indipendentemente da altri diritti, anche se vietano l'accesso in lettura a oggetti specifici.
Caratteristiche generali: **Funzionalità di base**	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Regole di spostamento dei dispositivi (creazione, modifica o eliminazione) per il server virtuale: **Scrittura**, **Esegui operazioni per le selezioni dispositivi** • Ottenere un certificato personalizzato per il protocollo Mobile (LWNGT): **Lettura** • Impostare un certificato personalizzato per il	• "Scarica aggiornamenti nell'archivio di Administration Server" • "Invia rapporti" • "Distribuisci pacchetto di installazione" • "Installa l'applicazione negli Administration Server	• "Rapporto sullo stato della protezione" • "Rapporto sulle minacce" • "Rapporto sui dispositivi più infetti" • "Rapporto sullo stato dei database anti-virus" • "Rapporto sugli errori"	None

		protocollo Mobile (LWNGT): **Scrittura** • Ottenere l'elenco di reti definito da NLA: **Lettura** • Aggiungere, modificare o eliminare l'elenco di reti definito da NLA: **Scrittura** • Visualizzare gli elenchi di controllo di accesso dei gruppi: **Lettura** • Visualizzare il registro del sistema operativo: **Lettura** • Visualizzare la chiave di ripristino per ripristinare l'accesso a un disco rigido con Crittografia unità BitLocker: **Esegui**	secondari in remoto"	• "Rapporto sugli attacchi di rete" • "Rapporto di riepilogo sulle applicazioni di difesa perimetrale installate" • "Rapporto di riepilogo sui tipi di applicazioni installate" • "Rapporto sugli utenti dei dispositivi infetti" • "Rapporto sugli incidenti" • "Rapporto sugli eventi" • "Rapporto sull'attività dei punti di distribuzione" • "Rapporto sugli Administration Server secondari" • "Rapporto sugli eventi di Controllo Dispositivi" • "Rapporto sulle applicazioni proibite" • "Rapporto su Controllo Web" • "Rapporto sullo stato di criptaggio dei dispositivi gestiti" • "Rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa" • "Rapporto sui diritti di accesso alle unità criptate" • "Rapporto sugli errori di criptaggio dei file" • "Rapporto sul blocco dell'accesso ai file criptati" • "Rapporto sulle autorizzazioni utente effettive" • "Rapporto sui diritti"	
Caratteristiche generali: **Oggetti eliminati**	• **Lettura** • **Scrittura**	• Visualizzare gli oggetti eliminati nel Cestino: **Lettura** • Eliminare gli oggetti dal Cestino: **Scrittura**	None	None	None
Caratteristiche generali:	• **Elimina eventi**	• Modificare le impostazioni di registrazione degli	None	None	Impostazioni: • Numero massimo di

Elaborazione degli eventi	• **Modifica impostazioni di notifica eventi** • **Modifica impostazioni registro eventi** • **Scrittura**	eventi: **Modifica impostazioni registro eventi** • Modificare le impostazioni di notifica degli eventi: **Modifica impostazioni di notifica eventi** • Eliminare gli eventi: **Elimina eventi**			eventi archiviati nel database • Periodo di tempo per l'archiviazione degli eventi dai dispositivi eliminati
Caratteristiche generali: **Operazioni in Administration Server**	• **Lettura** • **Scrittura** • **Esecuzione** • **Modifica elenchi di controllo degli accessi agli oggetti** • **Esegui operazioni per le selezioni dispositivi**	• Specificare le porte dell'Administration Server per la connessione di Network Agent: **Scrittura** • Specificare le porte del proxy di attivazione avviato sull'Administration Server: **Scrittura** • Specificare le porte del proxy di attivazione per i dispositivi mobili avviato sull'Administration Server: **Scrittura** • Specificare le porte del server Web per la distribuzione di pacchetti indipendenti: **Scrittura** • Specificare le porte del server Web per la distribuzione dei profili MDM: **Scrittura** • Specificare le porte SSL dell'Administration Server per la connessione tramite Web Console: **Scrittura** • Specificare le porte dell'Administration Server per la connessione mobile: **Scrittura** • Specificare il numero massimo di eventi archiviati nel database dell'Administration Server: **Scrittura** • Specificare il numero massimo di eventi che possono essere inviati dall'Administration Server: **Scrittura** • Specificare il periodo di tempo durante il quale gli eventi possono essere inviati dall'Administration Server: **Scrittura**	• "Backup dei dati di Administration Server" • "Manutenzione database"	None	None
Caratteristiche generali: **Distribuzione del software Kaspersky**	• **Gestisci patch di Kaspersky** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per**	Accettare o rifiutare l'installazione della patch: **Gestisci patch di Kaspersky**	None	• "Rapporto sull'utilizzo delle chiavi di licenza da parte dell'Administration Server virtuale" • "Rapporto sulle versioni del	Pacchetto di installazione: "Kaspersky"

	le selezioni dispositivi			software Kaspersky" • "Rapporto sulle applicazioni incompatibili" • "Rapporto sulle versioni degli aggiornamenti dei moduli software Kaspersky" • "Rapporto sulla distribuzione della protezione"	
Caratteristiche generali: **Gestione delle chiavi**	• **Esporta file chiave** • **Scrittura**	• Esportare il file chiave: **Esporta file chiave** • Modificare le impostazioni della chiave di licenza di Administration Server: **Scrittura**	None	None	None
Caratteristiche generali: **Gestione dei rapporti forzata**	• **Lettura** • **Scrittura**	• Creare rapporti indipendentemente dagli elenchi di controllo degli accessi degli oggetti: **Scrittura** • Eseguire rapporti indipendentemente dagli elenchi di controllo degli accessi degli oggetti: **Lettura**	None	None	None
Caratteristiche generali: **Gerarchia di Administration Server**	**Configura gerarchia di Administration Server**	• Registrare, aggiornare o eliminare gli Administration Server secondari: **Configura gerarchia di Administration Server**	None	None	None
Caratteristiche generali: **Autorizzazioni utente**	**Modifica elenchi di controllo degli accessi agli oggetti**	• Modificare le proprietà Protezione di qualsiasi oggetto: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire i ruoli utente: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire gli utenti interni: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire i gruppi di protezione: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire gli alias: **Modifica elenchi di controllo degli accessi agli oggetti**	None	None	None
Caratteristiche generali: **Administration Server virtuali**	• **Gestisci Administration Server virtuali** • **Lettura**	• Ottenere l'elenco degli Administration Server virtuali: **Lettura** • Ottenere informazioni sull'Administration	None	None	None

	• **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	Server virtuale: **Lettura** • Creare, aggiornare o eliminare un Administration Server virtuale: **Gestisci Administration Server virtuali** • Spostare un Administration Server virtuale in un altro gruppo: **Gestisci Administration Server virtuali** • Impostare le autorizzazioni dei server virtuali: **Gestisci Administration Server virtuali**			
Caratteristiche generali: **Gestione delle chiavi di criptaggio**	**Scrittura**	Importazione delle chiavi di criptaggio: **Scrittura**	None	None	None
Gestione sistema: **Vulnerability e patch management**	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Visualizzare le proprietà delle patch di terze parti: **Lettura** • Modificare le proprietà delle patch di terze parti: **Scrittura**	• "Correggi vulnerabilità" • "Installa aggiornamenti richiesti e correggi vulnerabilità"	"Rapporto sugli aggiornamenti software"	None

Ruoli utente predefiniti

I ruoli utente assegnati agli utenti di Kaspersky Security Center Linux forniscono set di diritti di accesso alle funzionalità dell'applicazione.

Agli utenti creati in un server virtuale non può essere assegnato un ruolo in Administration Server.

È possibile utilizzare i ruoli utente predefiniti con un set di diritti già configurato oppure creare nuovi ruoli. Quando si crea un nuovo ruolo, è necessario impostare l'ambito del ruolo e assegnare autonomamente i diritti di accesso alle funzionalità di Kaspersky Security Center Linux. Alcuni dei ruoli utente predefiniti disponibili in Kaspersky Security Center Linux possono essere associati a posizioni lavorative specifiche, ad esempio **Auditor**, **Addetto alla sicurezza** e **Supervisore**. I diritti di accesso di questi ruoli sono preconfigurati in base alle attività standard e all'ambito delle mansioni lavorative delle posizioni associate. La tabella seguente illustra il modo in cui è possibile associare i ruoli a posizioni specifiche.

Esempi di ruoli per posizioni specifiche

Ruolo	Commento
Auditor	Consente tutte le operazioni con tutti i tipi di rapporti, tutte le operazioni di visualizzazione, inclusa la visualizzazione degli oggetti eliminati (concede le autorizzazioni di **lettura** e **scrittura** nell'area **Oggetti eliminati**). Non consente altre operazioni. È possibile assegnare questo ruolo a una persona che esegue il controllo dell'organizzazione.
Supervisore	Consente tutte le operazioni di visualizzazione; non consente le altre operazioni. È possibile assegnare questo ruolo a un security officer e ad altri manager responsabili della sicurezza IT dell'organizzazione.
Security Officer	Consente tutte le operazioni di visualizzazione e la gestione dei rapporti; concede autorizzazioni limitate per l'area **Gestione sistema**: **Connettività**. È possibile assegnare questo ruolo a un addetto responsabile della sicurezza IT dell'organizzazione.

La tabella seguente illustra i diritti di accesso assegnati a ciascun ruolo utente predefinito.

Le caratteristiche delle aree funzionali **Mobile Device Management: Generale** e **Gestione sistema** non sono disponibili in Kaspersky Security Center Linux. Un utente con i ruoli amministratore/operatore di **Vulnerability e patch management** o **Amministratore/Operatore Mobile Device Management** hanno accesso solo per i diritti dell'area **Caratteristiche generali**: **Funzionalità di base**.

Diritti di accesso dei ruoli utente predefiniti

Ruolo	Descrizione
Amministratore Administration Server	Consente tutte le operazioni nelle seguenti aree funzionali, in **Caratteristiche generali**: • **Funzionalità di base** • **Elaborazione degli eventi** • **Gerarchia di Administration Server** • **Administration Server virtuali** Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.
Operatore Administration Server	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali, in **Caratteristiche generali**: • **Funzionalità di base** • **Administration Server virtuali**
Auditor	Consente tutte le operazioni nelle seguenti aree funzionali, in **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Oggetti eliminati** • **Gestione dei rapporti forzata** È possibile assegnare questo ruolo a una persona che esegue il controllo dell'organizzazione.
Amministratore installazione	Consente tutte le operazioni nelle seguenti aree funzionali, in **Caratteristiche generali**: • **Funzionalità di base** • **Distribuzione del software Kaspersky** • **Gestione delle chiavi di licenza** Concede i diritti **Lettura** ed **Esecuzione** nell'area funzionale **Caratteristiche generali: Administration Server virtuali**.
Operatore installazione	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali, in **Caratteristiche generali**: • **Funzionalità di base** • **Distribuzione del software Kaspersky** (concede anche il diritto **Gestisci patch di Kaspersky Lab** in quest'area) • **Administration Server virtuali**
Amministratore Kaspersky Endpoint Security	Consente tutte le operazioni nelle seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • Area Kaspersky Endpoint Security, incluse tutte le funzionalità Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.
Operatore Kaspersky Endpoint Security	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • Area Kaspersky Endpoint Security, incluse tutte le funzionalità
Amministratore principale	Consente tutte le operazioni nelle aree funzionali, *ad eccezione* delle seguenti aree, **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Gestione dei rapporti forzata** Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.
Operatore principale	Concede i diritti **Lettura** ed **Esecuzione** (ove applicabile) in tutte le seguenti aree funzionali: • **Caratteristiche generali**: • **Funzionalità di base** • **Oggetti eliminati** • **Operazioni in Administration Server** • **Distribuzione del software Kaspersky Lab**

	• **Administration Server virtuali** • Area Kaspersky Endpoint Security, incluse tutte le funzionalità
Amministratore Mobile Device Management	Consente tutte le operazioni nell'area funzionale **Caratteristiche generali: Funzionalità di base**.
Security Officer	Consente tutte le operazioni nelle seguenti aree funzionali, in **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Gestione dei rapporti forzata** Concede i diritti **Lettura**, **Scrittura**, **Esecuzione**, **Salva i file dei dispositivi nella workstation dell'amministratore** ed **Esegui operazioni per le selezioni di dispositivi** nell'area funzionale **Gestione sistema: Connettività**. È possibile assegnare questo ruolo a un addetto responsabile della sicurezza IT dell'organizzazione.
Utente del Portale Self Service	Consente tutte le operazioni nell'area funzionale **Mobile Device Management: Portale Self Service**. Questa funzionalità non è supportata in Kaspersky Security Center 11 e versioni successive.
Supervisore	Concede il diritto **Lettura** nelle aree funzionali **Caratteristiche generali**: **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** e **Caratteristiche generali**: **Gestione dei rapporti forzata**. È possibile assegnare questo ruolo a un security officer e ad altri manager responsabili della sicurezza IT dell'organizzazione.

Assegnazione dei diritti di accesso a oggetti specifici

Oltre ad assegnare diritti di accesso a livello di server, è possibile configurare l'accesso a oggetti specifici, ad esempio a un'attività specifica. L'applicazione consente di specificare i diritti di accesso per i seguenti tipi di oggetti:

- Gruppi di amministrazione
- Attività
- Rapporti
- Selezioni dispositivi
- Selezioni eventi

Per assegnare i diritti di accesso a un oggetto specifico:

1. In base al tipo di oggetto, nel menu principale passare alla sezione corrispondente:
   - **Risorse (dispositivi) → Gerarchia dei gruppi**
   - **Risorse (dispositivi) → Attività**
   - **Monitoraggio e generazione dei rapporti → Rapporti**
   - **Risorse (dispositivi) → Selezioni dispositivi**
   - **Monitoraggio e generazione dei rapporti → Selezioni eventi**
2. Aprire le proprietà dell'oggetto per il quale si desidera configurare i diritti di accesso.

   Per aprire la finestra delle proprietà di un gruppo di amministrazione o di un'attività, fare clic sul nome dell'oggetto. È possibile aprire le proprietà di altri oggetti utilizzando il pulsante sulla barra degli strumenti.

3. Nella finestra delle proprietà, aprire la sezione **Diritti di accesso**.

   Verrà visualizzato l'elenco di utenti. Gli utenti e i gruppi di protezione elencati dispongono dei diritti di accesso all'oggetto. Per impostazione predefinita, se si utilizza una gerarchia di gruppi di amministrazione o server, l'elenco e i diritti di accesso vengono ereditati dal gruppo di amministrazione principale o dal server primario.

4. Per poter modificare l'elenco, abilitare l'opzione **Usa autorizzazioni personalizzate**.

5. Configurare i diritti di accesso:

   - Utilizzare i pulsanti **Aggiungi** ed **Elimina** per modificare l'elenco.
   - Specificare i diritti di accesso per un utente o un gruppo di protezione. Eseguire una delle seguenti operazioni:
     - Se si desidera specificare i diritti di accesso manualmente, selezionare l'utente o il gruppo di protezione, fare clic sul pulsante **Diritti di accesso**, quindi specificare i diritti di accesso.
     - Se si desidera assegnare un ruolo utente all'utente o al gruppo di protezione, selezionare l'utente o il gruppo di protezione, fare clic sul pulsante **Ruoli** e selezionare il ruolo da assegnare.

6. Fare clic sul pulsante **Salva**.

I diritti di accesso all'oggetto sono configurati.

Assegnazione dei diritti di accesso a utenti e gruppi

È possibile concedere a utenti e gruppi di protezione i diritti di accesso per utilizzare diverse funzionalità di Administration Server, ad esempio, Kaspersky Endpoint Security for Linux.

Per assegnare i diritti di accesso a un utente o un gruppo di protezione:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Diritti di accesso**, selezionare la casella di controllo accanto al nome dell'utente o del gruppo di protezione a cui assegnare i diritti, quindi fare clic sul pulsante **Diritti di accesso**.

   Non è possibile selezionare più utenti o gruppi di sicurezza contemporaneamente. Se si selezionano più elementi, il pulsante **Diritti di accesso** verrà disabilitato.

3. Configurare il set di diritti per l'utente o il gruppo:

   a. Espandere il nodo con le funzionalità di Administration Server o di un'altra applicazione Kaspersky.

   b. Selezionare la casella di controllo **Consenti** o **Nega** accanto alla funzionalità o al diritto di accesso desiderato.

      Esempio 1: selezionare la casella di controllo **Consenti** accanto al nodo **Integrazione applicazione** per concedere tutti i diritti di accesso disponibili alla funzionalità di integrazione dell'applicazione (**Lettura**, **Scrittura** ed **Esecuzione**) per un utente o un gruppo.

      Esempio 2: espandere il nodo **Gestione chiavi di criptaggio**, quindi selezionare la casella di controllo **Consenti** accanto all'autorizzazione **Scrittura** per concedere il diritto di accesso in **scrittura** alla funzionalità di gestione delle chiavi di criptaggio per un utente o un gruppo.

4. Dopo aver configurato il set di diritti di accesso, fare clic su **OK**.

Verrà configurato il set di diritti per l'utente o il gruppo di utenti.

Le autorizzazioni dell'Administration Server (o del gruppo di amministrazione) sono suddivise nelle seguenti aree:

- Caratteristiche generali:
  - Gestione dei gruppi di amministrazione
  - Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi
  - Funzionalità di base
  - Oggetti eliminati
  - Gestione delle chiavi di criptaggio
  - Elaborazione degli eventi
  - Operazioni in Administration Server (solo nella finestra delle proprietà di Administration Server)
  - Tag dispositivo
  - Distribuzione del software Kaspersky
  - Gestione delle chiavi di licenza
  - Integrazione dell'applicazione
  - Gestione dei rapporti forzata
  - Gerarchia di Administration Server
  - Autorizzazioni utente
  - Administration Server virtuali
- Mobile Device Management:
  - Generale
  - Portale Self Service
- Gestione sistema:
  - Connettività
  - Inventario hardware
  - Controllo accesso alla rete (NAC)
  - Distribuzione del sistema operativo
  - Vulnerability e patch management

- Installazione remota
- Inventario software

Se non si seleziona **Consenti** o **Nega** per un diritto di accesso, il diritto di accesso viene considerato *non definita*: è negata finché non viene negata o consentita in modo esplicito per l'utente.

I diritti di un utente sono la somma di quanto segue:

- I diritti propri dell'utente
- I diritti di tutti i ruoli assegnati all'utente
- I diritti di tutto il gruppo di protezione a cui appartiene l'utente
- I diritti di tutti i ruoli assegnati ai gruppi di protezione a cui appartiene l'utente

Se almeno uno di questi set di diritti ha l'autorizzazione **Nega**, l'autorizzazione viene negata all'utente, anche se altri set la consentono o la lasciano non definita.

È inoltre possibile aggiungere utenti e gruppi di protezione all'ambito di un ruolo utente per usare funzionalità diverse di Administration Server. Le impostazioni associate a un ruolo utente si applicheranno solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Aggiunta di un account di un utente interno

Per aggiungere un nuovo account utente interno a Kaspersky Security Center Linux:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Aggiungi utente** visualizzata specificare le impostazioni del nuovo account utente:
   - **Nome**.
   - **Password** per la connessione dell'utente a Kaspersky Security Center Linux.
     La password deve rispettare le seguenti regole:
     - La password deve avere una lunghezza compresa tra 8 e 16 caratteri.
     - La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
       - Lettere maiuscole (A-Z)
       - Lettere minuscole (a-z)
       - Numeri (0-9)
       - Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

- La password non deve contenere spazi, caratteri Unicode o la combinazione di "." e "@", quando "." si trova prima di "@".

Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

Il numero di tentativi per l'immissione della password è limitato. Per impostazione predefinita, il numero massimo di tentativi di immissione della password consentiti è 10. È possibile modificare il numero di tentativi di immissione della password consentiti, come descritto in "Modifica del numero di tentativi di immissione della password consentiti".

Se l'utente raggiunge il numero di tentativi specificato per l'immissione della password, il relativo account viene bloccato per un'ora. È possibile sbloccare l'account utente solo modificando la password.

4. Fare clic su **Salva** per salvare le modifiche.

Un nuovo account di utenti viene aggiunto all'elenco di utenti.

Creazione di un gruppo di protezione

Per creare un gruppo di protezione:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Gruppi**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Crea gruppo di protezione** visualizzata, specificare le seguenti impostazioni per il nuovo gruppo di protezione:
   - **Nome gruppo**
   - **Descrizione**
4. Fare clic su **Salva** per salvare le modifiche.

Un nuovo gruppo di protezione viene aggiunto all'elenco dei gruppi.

Modifica di un account di un utente interno

Per modificare un account utente interno in Kaspersky Security Center Linux:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic sul nome dell'account utente che si desidera modificare.
3. Nella finestra delle impostazioni utente visualizzata, nella scheda **Generale**, modificare le impostazioni dell'account utente:

- **Descrizione**
- **Nome completo**
- **Indirizzo e-mail**
- **Telefono principale**
- **Imposta nuova password** per la connessione dell'utente a Kaspersky Security Center Linux.

  La password deve rispettare le seguenti regole:

  - La password deve avere una lunghezza compresa tra 8 e 16 caratteri.
  - La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
    - Lettere maiuscole (A-Z)
    - Lettere minuscole (a-z)
    - Numeri (0-9)
    - Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - La password non deve contenere spazi, caratteri Unicode o la combinazione di "." e "@", quando "." si trova prima di "@".

  Per visualizzare la password immessa, tenere premuto il pulsante **Mostra**.

  > Il numero di tentativi per l'immissione della password è limitato. Per impostazione predefinita, il numero massimo di tentativi di immissione della password consentiti è 10. È possibile modificare il numero di tentativi consentiti; tuttavia, per motivi di sicurezza, è consigliabile non ridurlo. Se l'utente raggiunge il numero di tentativi specificato per l'immissione della password, il relativo account viene bloccato per un'ora. È possibile sbloccare l'account utente solo modificando la password.

- Se necessario, spostare l'interruttore su **Disabilitato** per impedire all'utente di connettersi all'applicazione. È ad esempio possibile disabilitare un account dopo che un dipendente lascia l'azienda.

4. Nella scheda **Sicurezza in fase di autenticazione** è possibile specificare le impostazioni di protezione per questo account.
5. Nella scheda **Gruppi** è possibile aggiungere l'utente ai gruppi di protezione.
6. Nella scheda **Dispositivi** è possibile assegnare dispositivi all'utente.
7. Nella scheda **Ruoli** è possibile assegnare ruoli all'utente.
8. Fare clic su **Salva** per salvare le modifiche.

L'account utente aggiornato verrà visualizzato nell'elenco di utenti.

Modifica di un gruppo di protezione

Per modificare un gruppo di protezione:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Gruppi**.
2. Fare clic sul nome del gruppo di protezione che si desidera modificare.
3. Nella finestra delle impostazioni del gruppo visualizzata modificare le impostazioni del gruppo di protezione:
   - Nella scheda **Generale**, è possibile modificare le impostazioni **Nome** e **Descrizione**. Queste impostazioni sono disponibili solo per i gruppi di protezione interni.
   - Nella scheda **Utenti**, è possibile aggiungere utenti al gruppo di protezione. Questa impostazione è disponibile solo per utenti interni e gruppi di protezione interni.
   - Nella scheda **Ruoli**, è possibile assegnare un ruolo al gruppo di protezione.
4. Fare clic su **Salva** per salvare le modifiche.

Le modifiche vengono applicate al gruppo di protezione.

Assegnazione di un ruolo a un utente o un gruppo di protezione

Per assegnare un ruolo a un utente o un gruppo di protezione:

1. Nel menu principale, passare su **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti** o **Gruppi**.
2. Selezionare il nome dell'utente o del gruppo di protezione a cui assegnare un ruolo.

   È possibile selezionare più nomi.
3. Nella riga del menu fare clic sul pulsante **Assegna ruolo**.

   Verrà avviata l'Assegnazione guidata ruolo.
4. Seguire le istruzioni della procedura guidata: selezionare il ruolo che si desidera assegnare agli utenti o gruppi di protezione selezionati, quindi selezionare l'ambito del ruolo.

   Un *ambito di un ruolo utente* è una combinazione di utenti e gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Il ruolo con un set di diritti per l'utilizzo di Administration Server viene assegnato all'utente (o agli utenti o al gruppo di protezione). Nell'elenco degli utenti o dei gruppi di sicurezza, viene visualizzata una casella di controllo nella colonna **Ha ruoli assegnati**.

Aggiunta di account utente a un gruppo di protezione interno

È possibile aggiungere solo account di utenti interni a un gruppo di protezione interno.

Per aggiungere account utente a un gruppo di protezione interno:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Selezionare le caselle di controllo accanto agli account utente che si desidera aggiungere a un gruppo di protezione.
3. Fare clic sul pulsante **Assegna gruppo**.
4. Nella finestra **Assegna gruppo** visualizzata selezionare il gruppo di protezione a cui si desidera aggiungere gli account utente.
5. Fare clic sul pulsante **Salva**.

Gli account utente verranno aggiunti al gruppo di protezione. È inoltre possibile aggiungere utenti interni a un gruppo di protezione utilizzando le impostazioni del gruppo.

Assegnazione di un utente come proprietario dispositivo

Per informazioni sull'assegnazione di un utente come proprietario di un dispositivo mobile, vedere la Guida di Kaspersky Security for Mobile.

Per assegnare un utente come proprietario dispositivo:

1. Se si desidera assegnare un proprietario di un dispositivo connesso a un Administration Server virtuale, passare prima all'Administration Server virtuale:
   a. Nel menu principale, fare clic sull'icona a forma di freccia di espansione (›) a destra del nome corrente dell'Administration Server.
   b. Selezionare l'Administration Server desiderato.
2. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
   Verrà visualizzato un elenco di utenti. Se si è attualmente connessi a un Administration Server virtuale, l'elenco include gli utenti dell'Administration Server virtuale corrente e dell'Administration Server primario.
3. Fare clic sul nome dell'account utente che si desidera assegnare come proprietario dispositivo.
4. Nella finestra delle impostazioni utente visualizzata, selezionare la scheda **Dispositivi**.
5. Fare clic su **Aggiungi**.
6. Dall'elenco dei dispositivi selezionare il dispositivo che si desidera assegnare all'utente.
7. Fare clic su **OK**.

Il dispositivo selezionato verrà aggiunto all'elenco dei dispositivi assegnati all'utente.

È possibile eseguire la stessa operazione in **Risorse (dispositivi)** → **Dispositivi gestiti**, facendo clic sul nome del dispositivo che si desidera assegnare e quindi facendo clic sul collegamento **Gestisci proprietario dispositivo**.

Abilitazione della protezione dell'account dalle modifiche non autorizzate

È possibile abilitare un'opzione aggiuntiva per proteggere un account utente dalle modifiche non autorizzate. Se questa opzione è abilitata, la modifica delle impostazioni dell'account utente richiede l'autorizzazione dell'utente con i diritti di modifica.

Per abilitare o disabilitare la protezione dell'account dalle modifiche non autorizzate:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic sul nome dell'account utente interno per cui specificare la protezione dell'account dalle modifiche non autorizzate.
3. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Sicurezza in fase di autenticazione**.
4. Nella scheda **Sicurezza in fase di autenticazione**, selezionare l'opzione **Richiedi l'autenticazione per controllare l'autorizzazione di modifica di questo account** se si desidera richiedere le credenziali ogni volta che le impostazioni dell'account vengono modificate. In caso contrario, selezionare l'opzione **Consenti agli utenti di modificare questo account senza autenticazione aggiuntiva**.
5. Fare clic sul pulsante **Salva**.

Verifica in due passaggi

Questa sezione descrive come utilizzare la verifica in due passaggi per ridurre il rischio di accesso non autorizzato a Kaspersky Security Center Web Console.

Scenario: Configurazione della verifica in due passaggi per tutti gli utenti

Questo scenario descrive come abilitare la verifica in due passaggi per tutti gli utenti e come escludere gli account utente dalla verifica in due passaggi. Se non è stata abilitata la verifica in due passaggi per il proprio account prima di abilitarla per tutti gli altri utenti, l'applicazione apre innanzitutto la finestra per abilitare la verifica in due passaggi per il proprio account. Questo scenario descrive anche come abilitare la verifica in due passaggi per il proprio account.

> Se è stata abilitata la verifica in due passaggi per il proprio account, è possibile procedere al passaggio di abilitazione della verifica in due passaggi per tutti gli utenti.

Prerequisiti

Prima di iniziare:

- Assicurarsi che il proprio account utente disponga del diritto Modifica elenchi di controllo degli accessi agli oggetti dell'area funzionale **Caratteristiche generali: Autorizzazioni utente** per la modifica delle impostazioni di protezione per gli account di altri utenti.

- Assicurarsi che gli altri utenti di Administration Server installino un'app di autenticazione nei propri dispositivi.

Passaggi

L'abilitazione della verifica in due passaggi per tutti gli utenti procede per fasi:

1. **Installazione di un'app di autenticazione in un dispositivo**

   È possibile installare qualsiasi applicazione che supporti l'algoritmo TOTP (Time-based One-time Password), ad esempio:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex Key
   - Avanpost Authenticator
   - Aladdin 2FA

   Per verificare se Kaspersky Security Center Linux supporta l'app di autenticazione che si desidera utilizzare, abilitare la verifica in due passaggi per tutti gli utenti o per un determinato utente.

   Uno dei passaggi suggerisce di specificare il codice di sicurezza generato dall'app di autenticazione. In caso di esito positivo, Kaspersky Security Center Linux supporta l'applicazione di autenticazione selezionata.

   > Si sconsiglia vivamente di installare l'app di autenticazione nello stesso dispositivo da cui viene stabilita la connessione ad Administration Server.

2. **Sincronizzazione dell'ora dell'app di autenticazione con l'ora del dispositivo in cui è installato Administration Server**

   Verificare che l'ora nel dispositivo con l'app di autenticazione e l'ora nel dispositivo con Administration Server siano sincronizzate con UTC, utilizzando fonti orarie esterne. In caso contrario, potrebbero verificarsi errori durante l'autenticazione e l'attivazione della verifica in due passaggi.

3. **Abilitazione della verifica in due passaggi per il proprio account e ricezione della chiave segreta per il proprio account**

   Dopo aver abilitato la verifica in due passaggi per il proprio account, è possibile abilitare la verifica in due passaggi per tutti gli utenti.

4. **Abilitazione della verifica in due passaggi per tutti gli utenti**

   Gli utenti con la verifica in due passaggi abilitata devono utilizzarla per accedere ad Administration Server.

5. **Impedisci ai nuovi utenti di impostare la verifica in due passaggi per se stessi**

   Per migliorare ulteriormente la protezione dell'accesso a Kaspersky Security Center Web Console, è possibile impedire ai nuovi utenti di impostare autonomamente la verifica in due passaggi.

6. **Modifica del nome dell'emittente del codice di sicurezza**

   Se si dispone di più Administration Server con nomi simili, potrebbe essere necessario modificare i nomi dell'emittente del codice di sicurezza per un migliore riconoscimento dei diversi Administration Server.

7. **Esclusione degli account utente per cui non è necessario abilitare la verifica in due passaggi**

   Se necessario, è possibile escludere gli utenti dalla verifica in due passaggi. Gli utenti con account esclusi non devono utilizzare la verifica in due passaggi per accedere ad Administration Server.

8. **Configurazione della verifica in due passaggi per il proprio account**

   Se gli utenti non sono esclusi dalla verifica in due passaggi e la verifica in due passaggi non è ancora configurata per i propri account, è necessario configurarla nella finestra che si apre quando accedono a Kaspersky Security Center Web Console. In caso contrario, non saranno in grado di accedere ad Administration Server in base ai propri diritti.

Risultati

Al termine di questo scenario:

- La verifica in due passaggi è stata abilitata per l'account.
- La verifica in due passaggi è abilitata per tutti gli account utente di Administration Server, ad eccezione degli account utente che sono stati esclusi.

Informazioni sulla verifica in due passaggi per un account

Kaspersky Security Center Linux fornisce la verifica in due passaggi per gli utenti di Kaspersky Security Center Web Console. Quando la verifica in due passaggi è abilitata per il proprio account, ogni volta che si accede a Kaspersky Security Center Web Console è necessario immettere il nome utente, la password e un codice di sicurezza monouso aggiuntivo. Per ricevere un codice di sicurezza monouso è necessario disporre di un'app di autenticazione nel computer o nel dispositivo mobile.

Un codice di sicurezza ha un identificatore denominato *nome dell'emittente*. Il nome dell'emittente del codice di sicurezza viene utilizzato come identificatore di Administration Server nell'app di autenticazione. È possibile modificare il nome dell'emittente del codice di sicurezza. Il nome dell'emittente del codice di sicurezza ha un valore predefinito uguale al nome di Administration Server. Il nome dell'emittente viene utilizzato come identificatore di Administration Server nell'app di autenticazione. Se si modifica il nome dell'emittente del codice di sicurezza, è necessario emettere una nuova chiave segreta e passarla all'app di autenticazione. Un codice di sicurezza è monouso ed è valido per un massimo di 90 secondi (il tempo esatto può variare).

Qualsiasi utente per cui è abilitata la verifica in due passaggi può riemettere la propria chiave segreta. Quando un utente esegue l'autenticazione con la chiave segreta riemessa e la utilizza per l'accesso, Administration Server salva la nuova chiave segreta per l'account utente. Se l'utente immette la nuova chiave segreta in modo errato, Administration Server non salva la nuova chiave segreta e mantiene la chiave segreta corrente valida per l'ulteriore autorizzazione.

> Qualsiasi software di autenticazione che supporti l'algoritmo TOTP (Time-based One-time Password) può essere utilizzato come app di autenticazione, ad esempio Google Authenticator. Per generare il codice di sicurezza, è necessario sincronizzare l'ora impostata nell'app di autenticazione con l'ora impostata per Administration Server.

Per verificare se Kaspersky Security Center Linux supporta l'app di autenticazione che si desidera utilizzare, abilitare la verifica in due passaggi per tutti gli utenti o per un determinato utente.

Uno dei passaggi suggerisce di specificare il codice di sicurezza generato dall'app di autenticazione. In caso di esito positivo, Kaspersky Security Center Linux supporta l'applicazione di autenticazione selezionata.

Un'app di autenticazione genera il codice di sicurezza nel modo seguente:

1. Administration Server genera una chiave segreta speciale e un codice QR.
2. L'utente specifica la chiave segreta generata o il codice QR generato nell'app di autenticazione.
3. L'app di autenticazione genera un codice di sicurezza monouso che verrà specificato nella finestra di autenticazione di Administration Server.

Si consiglia vivamente di salvare la chiave segreta (o il codice QR) e conservarla in un luogo sicuro. Questo codice consentirà di ripristinare l'accesso a Kaspersky Security Center Web Console nel caso in cui si perda l'accesso al dispositivo mobile.

Per proteggere l'utilizzo di Kaspersky Security Center Linux, è possibile abilitare la verifica in due passaggi per il proprio account e abilitare la verifica in due passaggi per tutti gli utenti.

È possibile escludere gli account dalla verifica in due passaggi. Questa operazione può essere necessaria per gli account di servizio che non possono ricevere un codice di sicurezza per l'autenticazione.

La verifica in due passaggi funziona in base alle seguenti regole:

- Solo un account utente che dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente** può abilitare la verifica in due passaggi per tutti gli utenti.
- Solo un utente che ha abilitato la verifica in due passaggi per il proprio account può abilitare l'opzione di verifica in due passaggi per tutti gli utenti.
- Solo un utente che ha abilitato la verifica in due passaggi per il proprio account può escludere altri account utente dall'elenco della verifica in due passaggi abilitata per tutti gli utenti.
- Un utente può abilitare la verifica in due passaggi solo per il proprio account.
- Un account utente che dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente** e che ha eseguito l'accesso a Kaspersky Security Center Web Console utilizzando la verifica in due passaggi può disabilitare la verifica in due passaggi: per qualsiasi altro utente solo se la verifica in due passaggi per tutti gli utenti è disabilitata, per un utente escluso dall'elenco della verifica in due passaggi abilitata per tutti gli utenti.
- Qualsiasi utente che ha eseguito l'accesso a Kaspersky Security Center Web Console utilizzando la verifica in due passaggi può riemettere la propria chiave segreta.
- È possibile abilitare l'opzione di verifica in due passaggi per tutti gli utenti per l'Administration Server attualmente in uso. Se si abilita questa opzione in Administration Server, l'opzione viene abilitata anche per gli account utente dei relativi Administration Server virtuali e non si abilita la verifica in due passaggi per gli account utente degli Administration Server secondari.

Abilitazione della verifica in due passaggi per il proprio account

È possibile abilitare la verifica in due passaggi solo per il proprio account.

Prima di iniziare ad abilitare la verifica in due passaggi per il proprio account, assicurarsi che nel dispositivo mobile sia installata un'app di autenticazione. Assicurarsi che l'ora impostata nell'app di autenticazione sia sincronizzata con l'ora impostata nel dispositivo in cui è installato Administration Server.

Per abilitare la verifica in due passaggi per un account utente:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic sul nome dell'account.
3. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Sicurezza in fase di autenticazione**:
   a. Selezionare l'opzione **Richiedi nome utente, password e codice di sicurezza (verifica in due passaggi)**. Fare clic sul pulsante **Salva**.
   b. Nella finestra della verifica in due passaggi visualizzata, fare clic su **Visualizza come configurare la verifica in due passaggi**.
      Fare clic su **Visualizza codice QR.**
   c. Scansionare il codice QR dall'app di autenticazione sul dispositivo mobile per ricevere il codice di sicurezza monouso.
   d. Nella finestra della verifica in due passaggi specificare il codice di sicurezza generato dall'app di autenticazione, quindi fare clic sul pulsante **Controlla e applica**.
4. Fare clic sul pulsante **Salva**.

La verifica in due passaggi è stata abilitata per l'account.

Scansionare il codice QR dall'app di autenticazione sul dispositivo mobile per ricevere il codice di sicurezza monouso.

Abilitazione della verifica in due passaggi richiesta per tutti gli utenti

È possibile abilitare la verifica in due passaggi per tutti gli utenti di Administration Server se il proprio account dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente** e se è stata eseguita l'autenticazione utilizzando la verifica in due passaggi.

Per abilitare la verifica in due passaggi per tutti gli utenti:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.
   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Sicurezza in fase di autenticazione** della finestra delle proprietà spostare l'interruttore dell'opzione di **verifica in due passaggi per tutti gli utenti** sulla posizione "abilitato".
3. Se non è stata abilitata la verifica in due passaggi per il proprio account, l'applicazione apre la finestra per abilitare la verifica in due passaggi per il proprio account.

a. Nella finestra della verifica in due passaggi, fare clic su **Visualizza come configurare la verifica in due passaggi**.

b. Fare clic su **Visualizza codice QR.**

c. Scansionare il codice QR dall'applicazione di autenticazione sul dispositivo mobile per ricevere il codice di sicurezza monouso.

In alternativa, immettere manualmente la chiave segreta nell'applicazione di autenticazione.

d. Nella finestra della verifica in due passaggi specificare il codice di sicurezza generato dall'applicazione di autenticazione, quindi fare clic sul pulsante **Controlla e applica**.

La verifica in due passaggi è abilitata per tutti gli utenti. D'ora in poi gli utenti di Administration Server, inclusi gli utenti aggiunti dopo aver abilitato la verifica in due passaggi per tutti gli utenti, dovranno configurare la verifica in due passaggi per i propri account, ad eccezione degli utenti esclusi dalla verifica in due passaggi.

Disabilitazione della verifica in due passaggi per un account utente

È possibile disabilitare la verifica in due passaggi per il proprio account, nonché per l'account di un altro utente.

È possibile disabilitare la verifica in due passaggi di un altro account utente se il proprio account dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente** e se è stata eseguita l'autenticazione utilizzando la verifica in due passaggi.

Per disabilitare la verifica in due passaggi per un account utente:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic sul nome dell'account utente interno per cui si desidera disabilitare la verifica in due passaggi. Può trattarsi del proprio account o dell'account di un altro utente.
3. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Sicurezza in fase di autenticazione**.
4. Selezionare l'opzione **Richiedi solo nome utente e password** se si desidera disabilitare la verifica in due passaggi per un account utente.
5. Fare clic sul pulsante **Salva**.

La verifica in due passaggi è disabilitata per l'account utente.

Se si desidera ripristinare l'accesso per un utente che non può accedere a Kaspersky Security Center Web Console utilizzando la verifica in due passaggi, disabilitare la verifica in due passaggi per questo account utente, quindi selezionare l'opzione **Richiedi solo nome utente e password** come descritto sopra. Successivamente, accedere a Kaspersky Security Center Web Console con l'account utente per il quale è stata disabilitata la verifica in due passaggi, quindi abilitare nuovamente la verifica.

Disabilitazione della verifica in due passaggi richiesta per tutti gli utenti

È possibile disabilitare la verifica in due passaggi richiesta per tutti gli utenti se la verifica in due passaggi è abilitata per il proprio account e se quest'ultimo dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**. Se la verifica in due passaggi non è abilitata per il proprio account, è necessario abilitare la verifica in due passaggi per il proprio account prima di disabilitarla per tutti gli utenti.

Per disabilitare la verifica in due passaggi per tutti gli utenti:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Sicurezza in fase di autenticazione** della finestra delle proprietà spostare l'interruttore dell'opzione di **verifica in due passaggi per tutti gli utenti** sulla posizione "disabilitato".

3. Inserire le credenziali del proprio account nella finestra di autenticazione.

La verifica in due passaggi è disabilitata per tutti gli utenti. La disabilitazione della verifica in due passaggi per tutti gli utenti non si applica agli account specifici per i quali la verifica in due passaggi è stata precedentemente abilitata separatamente.

Esclusione di account dalla verifica in due passaggi

È possibile escludere gli account utente dalla verifica in due passaggi se si dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

Se un account utente viene escluso dall'elenco della verifica in due passaggi per tutti gli utenti, tale utente non deve utilizzare la verifica in due passaggi.

L'esclusione degli account dalla verifica in due passaggi può essere necessaria per gli account di servizio che non possono passare il codice di sicurezza durante l'autenticazione.

Se si desidera escludere alcuni account utente dalla verifica in due passaggi:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Sicurezza in fase di autenticazione** della finestra delle proprietà, nella tabella delle esclusioni dalla verifica in due passaggi fare clic sul pulsante **Aggiungi**.

3. Nella finestra visualizzata:

   a. Selezionare gli account utente che si desidera escludere.

   b. Fare clic sul pulsante **OK**.

Gli account utente selezionati vengono esclusi dalla verifica in due passaggi.

Configurazione della verifica in due passaggi per il proprio account

La prima volta che si accede a Kaspersky Security Center Linux dopo l'abilitazione della verifica in due passaggi, si apre la finestra per la configurazione della verifica in due passaggi per l'account.

Prima di configurare la verifica in due passaggi per il proprio account, assicurarsi che nel dispositivo mobile sia installata un'app di autenticazione. Verificare che l'ora nel dispositivo con l'app di autenticazione e l'ora nel dispositivo con Administration Server siano sincronizzate con UTC, utilizzando fonti orarie esterne.

Per configurare la verifica in due passaggi per il proprio account:

1. Generare un codice di sicurezza monouso utilizzando l'app di autenticazione sul dispositivo mobile. A tale scopo, eseguire una delle azioni seguenti:

   - Immettere manualmente la chiave segreta nell'app di autenticazione.
   - Fare clic su **Visualizza codice QR** ed eseguire la scansione del codice QR utilizzando l'app di autenticazione.

   Verrà visualizzato un codice di sicurezza sul dispositivo mobile.

2. Nella finestra di configurazione della verifica in due passaggi specificare il codice di sicurezza generato dall'app di autenticazione, quindi fare clic sul pulsante **Controlla e applica**.

La verifica in due passaggi viene configurata per il proprio account. È possibile accedere ad Administration Server in base ai propri diritti.

Impedisci ai nuovi utenti di impostare la verifica in due passaggi per se stessi

Per migliorare ulteriormente la protezione dell'accesso a Kaspersky Security Center Web Console, è possibile impedire ai nuovi utenti di impostare autonomamente la verifica in due passaggi.

Quando questa opzione è abilitata, un utente con la verifica in due passaggi disabilitata, ad esempio un nuovo amministratore di dominio, non può configurare autonomamente la verifica in due passaggi. Pertanto, tale utente non può essere autenticato in Administration Server e non può accedere a Kaspersky Security Center Web Console senza l'approvazione di un altro amministratore di Kaspersky Security Center Linux che ha già abilitato la verifica in due passaggi.

Questa opzione è disponibile se la verifica in due passaggi è abilitata per tutti gli utenti.

Per impedire ai nuovi utenti di impostare autonomamente la verifica in due passaggi:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Sicurezza in fase di autenticazione** della finestra delle proprietà, spostare l'interruttore **Vieta ai nuovi utenti di impostare la verifica in due passaggi per se stessi** nella posizione di abilitazione.

Questa opzione non influisce sugli account utente aggiunti alle esclusioni della verifica in due passaggi.

Per concedere a Kaspersky Security Center Web Console l'accesso a un utente con la verifica in due passaggi disabilitata, disattivare temporaneamente l'opzione **Vieta ai nuovi utenti di impostare la verifica in due passaggi per se stessi**, chiedere all'utente di abilitare la verifica in due passaggi, quindi riattivare l'opzione.

Generazione di una nuova chiave segreta

È possibile generare una nuova chiave segreta per la verifica in due passaggi per il proprio account solo se è stata eseguita l'autorizzazione utilizzando la verifica in due passaggi.

Per generare una nuova chiave segreta per un account utente:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic sul nome dell'account utente per cui si desidera generare una nuova chiave segreta per la verifica in due passaggi.
3. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Sicurezza in fase di autenticazione**.
4. Nella sceda **Sicurezza in fase di autenticazione**, fare clic sul collegamento **Genera una nuova chiave segreta**.
5. Nella finestra della verifica in due passaggi visualizzata specificare una nuova chiave di sicurezza generata dall'app di autenticazione.
6. Fare clic sul pulsante **Controlla e applica**.

Viene generata una nuova chiave segreta per l'utente.

Se il dispositivo mobile viene smarrito, è possibile installare un'app di autenticazione in un altro dispositivo mobile e generare una nuova chiave segreta per ripristinare l'accesso a Kaspersky Security Center Web Console.

Modifica del nome dell'emittente del codice di sicurezza

È possibile disporre di più identificatori (chiamati emittenti) per diversi Administration Server. È possibile modificare il nome dell'emittente di un codice di sicurezza ad esempio nel caso in cui Administration Server utilizzi già un nome simile dell'emittente del codice di sicurezza per un altro Administration Server. Per impostazione predefinita, il nome dell'emittente di un codice di sicurezza è uguale al nome di Administration Server.

Dopo aver modificato il nome dell'emittente del codice di sicurezza, è necessario riemettere una nuova chiave segreta e passarla all'app di autenticazione.

Per specificare un nuovo nome dell'emittente del codice di sicurezza:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Sicurezza in fase di autenticazione**.
3. Nella scheda **Sicurezza in fase di autenticazione**, fare clic sul collegamento **Modifica**.

   Verrà visualizzata la sezione **Modifica emittente codice di sicurezza**.

4. Specificare un nuovo nome dell'emittente del codice di sicurezza.

5. Fare clic sul pulsante **OK**.

Viene specificato un nuovo nome dell'emittente del codice di sicurezza per Administration Server.

Modifica del numero di tentativi di immissione della password consentiti

L'utente di Kaspersky Security Center Linux può immettere una password non valida un numero limitato di volte. Una volta raggiunto il limite, l'account utente viene bloccato per un'ora.

Per impostazione predefinita, il numero massimo di tentativi di immissione della password consentiti è 10. È possibile modificare il numero di tentativi di immissione della password consentiti, come descritto in questa sezione.

Per modificare il numero di tentativi di immissione della password consentiti:

1. Nel dispositivo Administration Server, eseguire una riga di comando Linux.

2. Per l'utilità klscflag, eseguire il seguente comando:

   ```
   sudo /opt/kaspersky/ksc64/sbin/klscflag -fset -pv klserver -n SrvSplPpcLogonAttempts -t d -v N
   ```

   dove N è un numero di tentativi di immissione di una password.

3. Per applicare le modifiche, riavviare il servizio Administration Server.

Il numero massimo di tentativi di immissione della password consentiti è stato modificato.

Eliminazione di un utente o un gruppo di protezione

È possibile eliminare solo utenti interni o gruppi di protezione interni.

Per eliminare un utente o un gruppo di protezione:

1. Nel menu principale, passare su **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti** o **Gruppi**.

2. Selezionare la casella di controllo accanto all'utente o al gruppo di protezione che si desidera eliminare.

3. Fare clic su **Elimina**.

4. Nella finestra visualizzata fare clic su **OK**.

L'utente o il gruppo di protezione verrà eliminato.

Creazione di un ruolo utente

Per creare un ruolo utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Nome nuovo ruolo** visualizzata immettere il nome del nuovo ruolo.
4. Fare clic su **OK** per applicare le modifiche.
5. Nella finestra delle proprietà del ruolo visualizzata modificare le impostazioni del ruolo:
   - Nella scheda **Generale** modificare il nome del ruolo.
     Non è possibile modificare il nome di un ruolo predefinito.
   - Nella scheda **Impostazioni** modificare l'ambito del ruolo, i criteri e i profili associati al ruolo.
   - Nella scheda **Diritti di accesso** modificare i diritti per l'accesso alle applicazioni Kaspersky.
6. Fare clic su **Salva** per salvare le modifiche.

Il nuovo ruolo verrà visualizzato nell'elenco dei ruoli utente.

Modifica di un ruolo utente

Per modificare un ruolo utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Fare clic sul nome del ruolo che si desidera modificare.
3. Nella finestra delle proprietà del ruolo visualizzata modificare le impostazioni del ruolo:
   - Nella scheda **Generale** modificare il nome del ruolo.
     Non è possibile modificare il nome di un ruolo predefinito.
   - Nella scheda **Impostazioni** modificare l'ambito del ruolo, i criteri e i profili associati al ruolo.
   - Nella scheda **Diritti di accesso** modificare i diritti per l'accesso alle applicazioni Kaspersky.
4. Fare clic su **Salva** per salvare le modifiche.

Il ruolo aggiornato verrà visualizzato nell'elenco dei ruoli utente.

Modifica dell'ambito di un ruolo utente

Un *ambito di un ruolo utente* è una combinazione di utenti e gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Per aggiungere utenti, gruppi di protezione e gruppi di amministrazione all'ambito di un ruolo utente, è possibile utilizzare una dei seguenti metodi:

Metodo 1:

1. Nel menu principale, passare su **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti** o **Gruppi**.
2. Selezionare le caselle di controllo accanto agli utenti o ai gruppi di protezione che si desidera aggiungere all'ambito del ruolo utente.
3. Fare clic sul pulsante **Assegna ruolo**.

   Verrà avviata l'Assegnazione guidata ruolo. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
4. Nel passaggio **Selezionare un ruolo** selezionare il ruolo utente che si desidera assegnare.
5. Nel passaggio **Definire l'ambito** selezionare il gruppo di amministrazione da aggiungere all'ambito del ruolo utente.
6. Fare clic sul pulsante **Assegna ruolo** per chiudere la finestra.

Gli utenti o i gruppi di protezione selezionati e il gruppo di amministrazione selezionato verranno aggiunti all'ambito del ruolo utente.

Metodo 2:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Fare clic sul nome del ruolo per cui si desidera definire l'ambito.
3. Nella finestra delle proprietà del ruolo visualizzata, selezionare la scheda **Impostazioni**.
4. Nella sezione **Ambito ruolo** fare clic su **Aggiungi**.

   Verrà avviata l'Assegnazione guidata ruolo. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
5. Nel passaggio **Definire l'ambito** selezionare il gruppo di amministrazione da aggiungere all'ambito del ruolo utente.
6. Nel passaggio **Selezionare gli utenti** della procedura guidata selezionare gli utenti e i gruppi di protezione che si desidera aggiungere all'ambito del ruolo utente.
7. Fare clic sul pulsante **Assegna ruolo** per chiudere la finestra.
8. Fare clic sul pulsante **Chiudi** (×) per chiudere la finestra delle proprietà del ruolo.

Gli utenti o i gruppi di protezione selezionati e il gruppo di amministrazione selezionato verranno aggiunti all'ambito del ruolo utente.

Metodo 3:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Diritti di accesso**, selezionare la casella di controllo accanto al nome dell'utente o del gruppo di sicurezza che si desidera aggiungere all'ambito dei ruoli utente, quindi fare clic sul pulsante **Ruoli**.

Non è possibile selezionare più utenti o gruppi di sicurezza contemporaneamente. Se si selezionano più elementi, il pulsante **Ruoli** verrà disabilitato.

3. Nella finestra **Ruoli** selezionare il ruolo utente che si desidera assegnare, quindi applicare e salvare le modifiche.

   Gli utenti o i gruppi di protezione selezionati verranno aggiunti all'ambito del ruolo utente.

Eliminazione di un ruolo utente

Per eliminare un ruolo utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Selezionare la casella di controllo accanto al nome del ruolo che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Nella finestra visualizzata fare clic su **OK**.

Il ruolo utente verrà eliminato.

Associazione dei profili criterio ai ruoli

È possibile associare i ruoli utente ai profili criterio. In questo caso, la regola di attivazione per questo profilo criterio si basa sul ruolo: il profilo criterio diventa attivo per un utente che ha il ruolo specificato.

Il criterio vieta ad esempio un software di navigazione GPS in tutti i dispositivi in un gruppo di amministrazione. Il software di navigazione GPS è necessario in un solo dispositivo nel gruppo di amministrazione Utenti: quello di proprietà di un corriere. In questo caso, è possibile assegnare un ruolo "Corriere" al proprietario, quindi creare un profilo criterio che consente l'esecuzione del software di navigazione GPS solo nei dispositivi i cui proprietari hanno il ruolo "Corriere". Tutte le altre impostazioni del criterio vengono mantenute. Solo l'utente con il ruolo "Corriere" sarà autorizzato a eseguire il software di navigazione GPS. Se in seguito viene assegnato il ruolo "Corriere" a un altro dipendente, anche il nuovo dipendente potrà eseguire il software di navigazione nel dispositivo dell'organizzazione. L'esecuzione del software di navigazione GPS sarà ancora non consentita negli altri dispositivi dello stesso gruppo di amministrazione.

Per associare un ruolo a un profilo criterio:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Fare clic sul nome del ruolo che si desidera associare a un profilo criterio.

   Verrà visualizzata la finestra delle proprietà del ruolo, con la scheda **Generale** selezionata.
3. Selezionare la scheda **Impostazioni** e scorrere fino alla sezione **Criteri e profili**.
4. Fare clic su **Modifica**.
5. Per associare il ruolo a:

   - **Un profilo criterio esistente**: fare clic sull'icona della freccia di espansione (>) accanto al nome del criterio desiderato, quindi selezionare la casella di controllo accanto al profilo a cui associare il ruolo.

- **Un nuovo profilo criterio**:

  a. Selezionare la casella di controllo accanto al criterio per cui si desidera creare un profilo.

  b. Fare clic su **Nuovo profilo criterio**.

  c. Specificare un nome per il nuovo profilo e configurare le impostazioni del profilo.

  d. Fare clic sul pulsante **Salva**.

  e. Selezionare la casella di controllo accanto al nuovo profilo.

6. Fare clic su **Assegna al ruolo**.

Il profilo verrà associato al ruolo e visualizzato nelle proprietà del ruolo. Il profilo si applica automaticamente a qualsiasi dispositivo il cui proprietario è assegnato al ruolo.

Propagazione dei ruoli utente agli Administration Server secondari

Per impostazione predefinita, gli elenchi dei ruoli utente degli Administration Server primari e secondari sono indipendenti. È possibile configurare l'applicazione in modo da propagare automaticamente i ruoli utente creati nell'Administration Server primario a tutti gli Administration Server secondari. I ruoli utente possono inoltre essere propagati da un Administration Server secondario ai relativi Administration Server secondari.

Per propagare i ruoli utente dall'Administration Server primario agli Administration Server secondari:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server, con la scheda **Generale** selezionata.

2. Passare alla sezione **Gerarchia di Administration Server**.

3. Abilitare l'opzione **Trasferisci elenco dei ruoli agli Administration Server secondari**, quindi fare clic sul pulsante **Salva**.

L'applicazione copierà i ruoli utente dell'Administration Server primario negli Administration Server secondari.

Quando l'opzione **Trasferisci elenco dei ruoli agli Administration Server secondari** è abilitata e vengono propagati i ruoli utente, questi non possono essere modificati o eliminati negli Administration Server secondari. Quando si crea un nuovo ruolo o si modifica un ruolo esistente nell'Administration Server primario, le modifiche vengono copiate automaticamente negli Administration Server secondari. Quando si elimina un ruolo utente nell'Administration Server primario, questo ruolo rimane negli Administration Server secondari, ma può essere modificato o eliminato.

I ruoli propagati all'Administration Server secondario dal server primario sono visualizzati con i segni di spunta verdi ( ). Non è possibile modificare tali ruoli nell'Administration Server secondario.

Se si crea un ruolo nell'Administration Server primario ed è presente un ruolo con lo stesso nome nell'Administration Server secondario, il nuovo ruolo viene copiato nell'Administration Server secondario con l'aggiunta di un indice al nome, ad esempio ~~1, ~~2 (l'indice può essere casuale).

Se si disabilita l'opzione **Trasferisci elenco dei ruoli agli Administration Server secondari**, tutti i ruoli utente restano negli Administration Server secondari, ma diventano indipendenti da quelli nell'Administration Server primario. Dopo essere diventati indipendenti, i ruoli utente negli Administration Server secondari possono essere modificati o eliminati.

Aggiornamento di database e applicazioni Kaspersky

Questa sezione descrive i passaggi da eseguire per aggiornare periodicamente i seguenti elementi:

- Database e moduli del software Kaspersky
- Applicazioni Kaspersky installate, inclusi i componenti di Kaspersky Security Center Linux e le applicazioni di protezione

Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Scenario: Aggiornamento periodico di database e applicazioni Kaspersky

Questa sezione fornisce uno scenario per l'aggiornamento periodico dei database, dei moduli software e delle applicazioni Kaspersky. Dopo aver completato lo scenario Configurazione della protezione di rete, è necessario mantenere l'affidabilità del sistema di protezione per assicurarsi che gli Administration Server e i dispositivi gestiti siano protetti da varie minacce, inclusi virus, attacchi di rete e attacchi di phishing.

La protezione della rete viene mantenuta aggiornata tramite aggiornamenti periodici dei seguenti elementi:

- Database e moduli del software Kaspersky
- Applicazioni Kaspersky installate, inclusi i componenti di Kaspersky Security Center Linux e le applicazioni di protezione

Completando questo scenario, è possibile avere la certezza di quanto segue:

- La rete è protetta dal software Kaspersky più recente, inclusi i componenti di Kaspersky Security Center Linux e le applicazioni di protezione.
- I database anti-virus e gli altri database Kaspersky di importanza critica per la sicurezza della rete sono sempre aggiornati.

Prerequisiti

I dispositivi gestiti devono disporre di una connessione ad Administration Server. Se non dispongono di una connessione, valutare se eseguire l'aggiornamento dei database e dei moduli software Kaspersky manualmente o direttamente dai server di aggiornamento Kaspersky.

Administration Server deve disporre di una connessione a Internet.

Prima di iniziare, verificare di avere:

1. Distribuito le applicazioni di protezione Kaspersky nei dispositivi gestiti in base allo scenario di distribuzione delle applicazioni Kaspersky tramite Kaspersky Security Center Web Console.
2. Creato e configurato tutti i criteri, i profili criterio e le attività richiesti in base allo scenario di configurazione della protezione di rete.

3. Assegnato un numero appropriato di punti di distribuzione in base al numero di dispositivi gestiti e alla topologia della rete.

L'aggiornamento dei database e delle applicazioni Kaspersky prevede diversi passaggi:

1. **Scelta di uno schema di aggiornamento**

   Esistono diversi schemi che è possibile utilizzare per installare gli aggiornamenti per le applicazioni di protezione. Scegliere lo schema o gli schemi più appropriati per i requisiti della rete.

2. **Creazione dell'attività per il download degli aggiornamenti nell'archivio di Administration Server**

   Questa attività viene creata automaticamente dall'avvio rapido guidato di Kaspersky Security Center. Se la procedura guidata non è stata eseguita, creare l'attività ora.

   Questa attività è necessaria per scaricare gli aggiornamenti dai server di aggiornamento Kaspersky nell'archivio di Administration Server, nonché per aggiornare i database e i moduli software Kaspersky per Kaspersky Security Center Linux. Dopo aver scaricato gli aggiornamenti, questi possono essere propagati ai dispositivi gestiti.

   Se nella rete sono stati assegnati punti di distribuzione, gli aggiornamenti vengono scaricati automaticamente dall'archivio di Administration Server agli archivi dei punti di distribuzione. In questo caso, i dispositivi gestiti inclusi nell'ambito di un punto di distribuzione scaricano gli aggiornamenti dall'archivio del punto di distribuzione anziché dall'archivio di Administration Server.

   Istruzioni dettagliate: Creazione dell'attività per il download degli aggiornamenti nell'archivio di Administration Server

3. **Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione (facoltativo)**

   Per impostazione predefinita, gli aggiornamenti vengono scaricati nei punti di distribuzione dall'Administration Server. È possibile configurare Kaspersky Security Center Linux per scaricare gli aggiornamenti nei punti di distribuzione direttamente dai server di aggiornamento Kaspersky. Il download negli archivi dei punti di distribuzione è preferibile se il traffico tra Administration Server e punti di distribuzione è superiore rispetto a quello del traffico tra i punti di distribuzione e i server di aggiornamento Kaspersky oppure se Administration Server non dispone di accesso a Internet.

   Quando nella rete sono stati assegnati punti di distribuzione ed è stata creata l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, i punti di distribuzione scaricano gli aggiornamenti dai server di aggiornamento Kaspersky e non dall'archivio dell'Administration Server.

   Istruzioni dettagliate: Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione

4. **Configurazione dei punti di distribuzione**

   Quando nella rete sono stati assegnati punti di distribuzione, verificare che l'opzione **Distribuisci aggiornamenti** sia abilitata nelle proprietà di tutti i punti di distribuzione richiesti. Quando questa opzione è disabilitata per un punto di distribuzione, i dispositivi inclusi nell'ambito del punto di distribuzione scaricano gli aggiornamenti dall'archivio di Administration Server.

5. **Ottimizzazione del processo di aggiornamento utilizzando i file diff (opzionale)**

   È possibile ottimizzare il traffico tra l'Administration Server e i dispositivi gestiti utilizzando i file diff. Quando questa funzionalità è abilitata, Administration Server o un punto di distribuzione scarica file diff anziché interi file di database o moduli software Kaspersky. Un file diff descrive le differenze tra due versioni di un file di un database o un modulo software. Pertanto, un file diff occupa meno spazio di un intero file. Questo comporta una riduzione del traffico tra Administration Server o i punti di distribuzione e i dispositivi gestiti. Per utilizzare questa funzionalità, abilitare l'opzione **Scarica file diff** nelle proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* e/o dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

   Istruzioni dettagliate: Utilizzo dei file diff per l'aggiornamento dei database e dei moduli del software Kaspersky

6. **Configurazione dell'installazione automatica degli aggiornamenti per le applicazioni di protezione**

Creare le attività di *aggiornamento* per le applicazioni gestite per garantire aggiornamenti tempestivi ai moduli software e ai database Kaspersky, inclusi i database anti-virus. Per garantire aggiornamenti tempestivi, è consigliabile selezionare l'opzione **Quando vengono scaricati nuovi aggiornamenti nell'archivio** durante la configurazione della pianificazione dell'attività.

Se la rete include dispositivi solo IPv6 e si desidera aggiornare regolarmente le applicazioni di protezione installate in tali dispositivi, assicurarsi che Administration Server versione 13.2 e Network Agent versione 13.2 siano installati nei dispositivi gestiti.

Se un aggiornamento richiede la visualizzazione e l'accettazione dei termini del Contratto di licenza con l'utente finale, è prima necessario accettare i termini. Successivamente, l'aggiornamento può essere propagato ai dispositivi gestiti.

Risultati

Al termine dello scenario, Kaspersky Security Center Linux è configurato per l'aggiornamento dei database Kaspersky dopo il download degli aggiornamenti nell'archivio di Administration Server. È quindi possibile procedere al monitoraggio dello stato della rete.

Informazioni sull'aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky

Per assicurarsi che la protezione dei propri Administration Server e dispositivi gestiti sia aggiornata, è necessario garantire aggiornamenti tempestivi dei seguenti componenti:

- Database e moduli del software Kaspersky

  Prima di scaricare i database e i moduli software di Kaspersky, Kaspersky Security Center Linux verifica se i server Kaspersky sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici. Ciò è necessario per garantire che i database anti-virus siano aggiornati e per mantenere il livello di sicurezza per i dispositivi gestiti.

- Applicazioni Kaspersky installate, inclusi i componenti di Kaspersky Security Center Linux e le applicazioni di protezione

  Kaspersky Security Center Linux non può aggiornare automaticamente le applicazioni Kaspersky. Per aggiornare le applicazioni, scaricare le versioni più recenti delle applicazioni dal sito Web di Kaspersky, quindi installarle manualmente:

  - Kaspersky Security Center Linux Administration Server, Kaspersky Security Center Web Console
  - Network Agent, Kaspersky Endpoint Security, plug-in Web di gestione

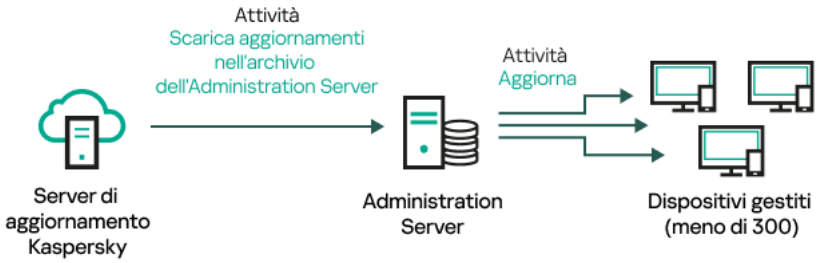
In base alla configurazione della propria rete è possibile utilizzare i seguenti schemi di download e distribuzione degli aggiornamenti richiesti ai dispositivi gestiti:

- Utilizzando un'unica attività: *Scarica aggiornamenti nell'archivio dell'Administration Server*
- Utilizzando due attività:
  - L'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*
  - L'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*

- Manualmente attraverso una cartella locale, una cartella condivisa o un server FTP
- Direttamente dai server di aggiornamento Kaspersky a Kaspersky Endpoint Security nei dispositivi gestiti
- Tramite una cartella locale o di rete se Administration Server non dispone della connessione a Internet

Utilizzo dell'attività Scarica aggiornamenti nell'archivio dell'Administration Server

In questo schema Kaspersky Security Center Linux scarica gli aggiornamenti tramite l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. Nelle reti piccole che contengono meno di 300 dispositivi gestiti in un singolo segmento di rete o meno di 10 dispositivi gestiti in ciascun segmento di rete, gli aggiornamenti vengono distribuiti nei dispositivi gestiti direttamente dall'archivio di Administration Server (vedere la figura di seguito).



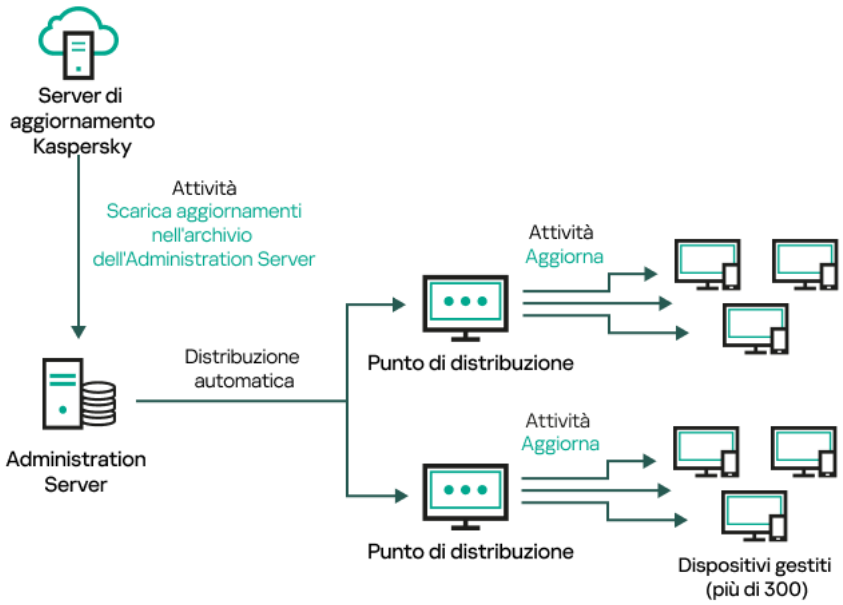
Aggiornamento tramite l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* senza punti di distribuzione

Come sorgente degli aggiornamenti, è possibile utilizzare non solo i server di aggiornamento Kaspersky, ma anche una cartella locale o di rete.

Per impostazione predefinita, Administration Server comunica con i server di aggiornamento Kaspersky e scarica gli aggiornamenti utilizzando il protocollo HTTPS. È possibile configurare Administration Server per fare in modo che utilizzi il protocollo HTTP anziché HTTPS.

Se la rete contiene 300 o più dispositivi gestiti in un singolo segmento di rete o se la rete è composta da più segmenti di rete con più di 9 dispositivi gestiti in ciascun segmento di rete, è consigliabile utilizzare i punti di distribuzione per propagare gli aggiornamenti ai dispositivi gestiti (vedere la figura di seguito). I punti di distribuzione riducono il carico per Administration Server e ottimizzano il traffico tra Administration Server e dispositivi gestiti. È possibile calcolare il numero e la configurazione dei punti di distribuzione richiesti per la rete.

In questo schema gli aggiornamenti vengono scaricati automaticamente dall'archivio di Administration Server agli archivi dei punti di distribuzione. I dispositivi gestiti inclusi nell'ambito di un punto di distribuzione scaricano gli aggiornamenti dall'archivio del punto di distribuzione anziché dall'archivio di Administration Server.



Aggiornamento tramite l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* con punti di distribuzione

Al completamento dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, gli aggiornamenti per i database e i moduli software Kaspersky per Kaspersky Endpoint Security vengono scaricati nell'archivio di Administration Server. Questi aggiornamenti vengono installati tramite l'attività di *aggiornamento* per Kaspersky Endpoint Security.

L'attività *Scarica aggiornamenti nell'archivio di Administration Server* non è disponibile negli Administration Server virtuali. L'archivio dell'Administration Server virtuale visualizza gli aggiornamenti scaricati nell'Administration Server primario.

È possibile configurare la verifica della possibilità di utilizzare gli aggiornamenti e degli eventuali errori in un set di dispositivi di test. Se la verifica ha esito positivo, gli aggiornamenti vengono distribuiti agli altri dispositivi gestiti.

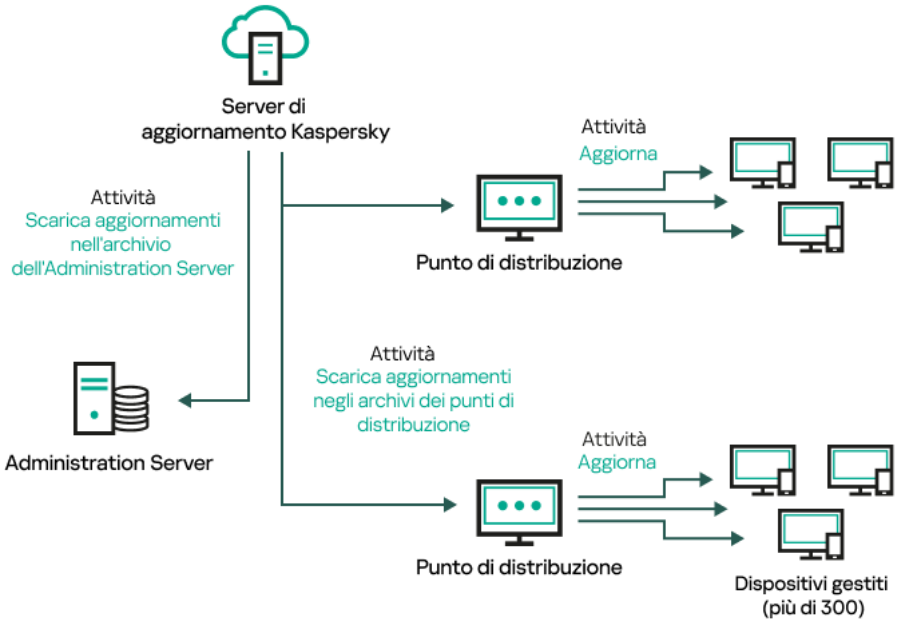
Ogni applicazione Kaspersky richiede gli aggiornamenti necessari da Administration Server. Administration Server aggrega tali richieste e scarica solo gli aggiornamenti che sono richiesti da un'applicazione. Questo garantisce che gli stessi aggiornamenti non vengano scaricati più volte e che gli aggiornamenti non necessari non vengano scaricati affatto. Durante l'esecuzione dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, Administration Server invia automaticamente le seguenti informazioni ai server di aggiornamento Kaspersky per garantire il download delle versioni appropriate dei moduli software e dei database Kaspersky:

- Versione e ID applicazione
- ID di installazione dell'applicazione
- ID chiave attiva
- ID di esecuzione dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*

Le informazioni trasmesse non contengono dati personali o altri dati riservati. AO Kaspersky Lab protegge le informazioni in base ai requisiti previsti dalla legge.

Tramite due attività: l'attività Scarica aggiornamenti nell'archivio dell'Administration Server e l'attività Scarica aggiornamenti negli archivi dei punti di distribuzione

È possibile scaricare gli aggiornamenti negli archivi dei punti di distribuzione direttamente dai server di aggiornamento Kaspersky anziché dall'archivio di Administration Server, quindi distribuire gli aggiornamenti ai dispositivi gestiti (vedere la figura di seguito). Il download negli archivi dei punti di distribuzione è preferibile se il traffico tra Administration Server e punti di distribuzione è superiore rispetto a quello del traffico tra i punti di distribuzione e i server di aggiornamento Kaspersky oppure se Administration Server non dispone di accesso a Internet.



Aggiornamento tramite l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* e l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*

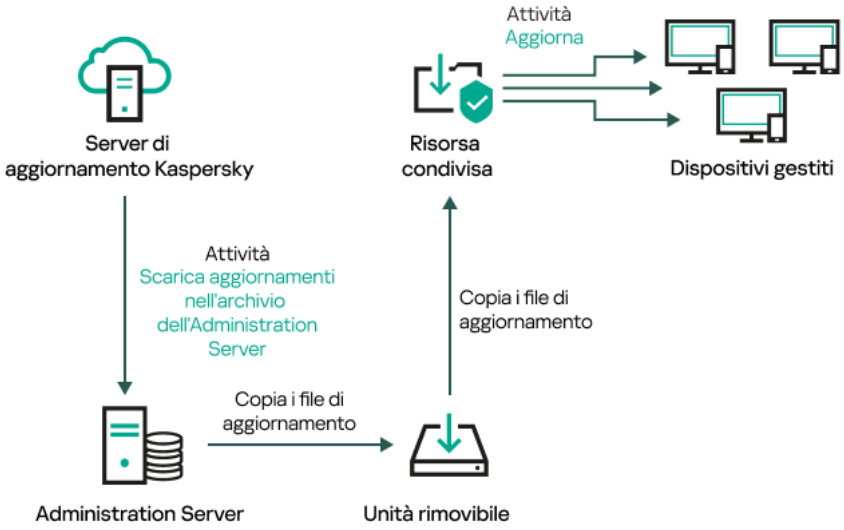
Per impostazione predefinita, Administration Server e i punti di distribuzione comunicano con i server di aggiornamento Kaspersky e scaricano gli aggiornamenti utilizzando il protocollo HTTPS. È possibile configurare Administration Server e/o i punti di distribuzione per fare in modo che utilizzino il protocollo HTTP anziché HTTPS.

Per implementare questo schema, creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* oltre all'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. In seguito, i punti di distribuzione scaricheranno gli aggiornamenti dai server di aggiornamento Kaspersky e non dall'archivio di Admnistration Server.

Anche l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* è richiesta per questo schema, poiché questa attività è utilizzata per scaricare i moduli software e i database Kaspersky per Kaspersky Security Center Linux.

Manualmente attraverso una cartella locale, una cartella condivisa o un server FTP

Se i dispositivi client non hanno una connessione ad Administration Server, è possibile utilizzare una cartella locale o una risorsa condivisa come sorgente per l'aggiornamento di database, moduli software e applicazioni Kaspersky. In questo schema è necessario copiare gli aggiornamenti richiesti dall'archivio di Administration Server in un'unità rimovibile, quindi copiare gli aggiornamenti nella cartella locale o nella risorsa condivisa specificata come sorgente degli aggiornamenti nelle impostazioni di Kaspersky Endpoint Security (vedere la figura di seguito).



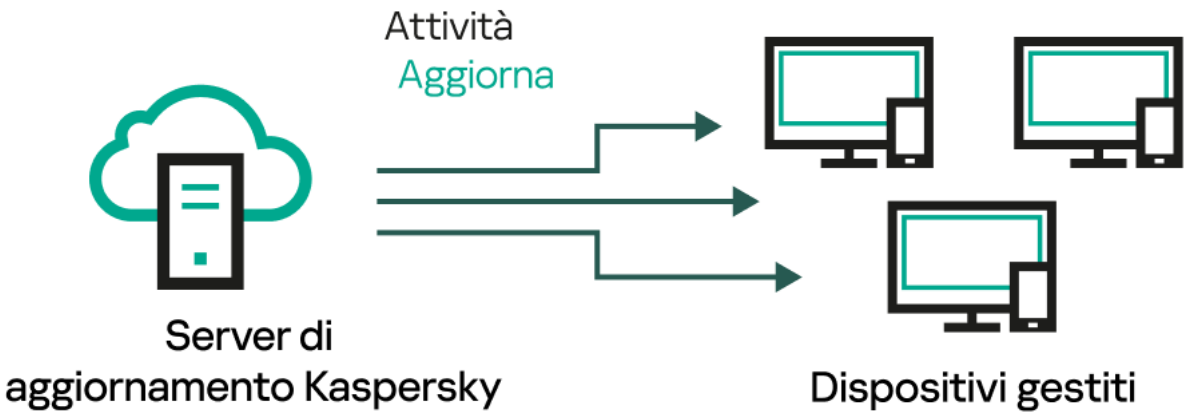
Aggiornamento tramite una cartella locale, una cartella condivisa o un server FTP

Per ulteriori informazioni sulle sorgenti degli aggiornamenti in Kaspersky Endpoint Security, consultare le seguenti Guide:

- Guida di Kaspersky Endpoint Security for Linux
- Guida di Kaspersky Endpoint Security for Windows

Direttamente dai server di aggiornamento Kaspersky a Kaspersky Endpoint Security nei dispositivi gestiti

Nei dispositivi gestiti, è possibile configurare Kaspersky Endpoint Security per ricevere gli aggiornamenti direttamente dai server di aggiornamento Kaspersky (vedere la figura di seguito).



Aggiornamento delle applicazioni di protezione direttamente dai server di aggiornamento Kaspersky

In questo schema, l'applicazione di protezione non utilizza l'archivio fornito da Kaspersky Security Center Linux. Per ricevere gli aggiornamenti direttamente dai server di aggiornamento Kaspersky, specificare i server di aggiornamento Kaspersky come sorgente degli aggiornamenti nell'applicazione di protezione. Per ulteriori informazioni su queste impostazioni, consultare le seguenti Guide:

- Guida di Kaspersky Endpoint Security for Linux
- Guida di Kaspersky Endpoint Security for Windows

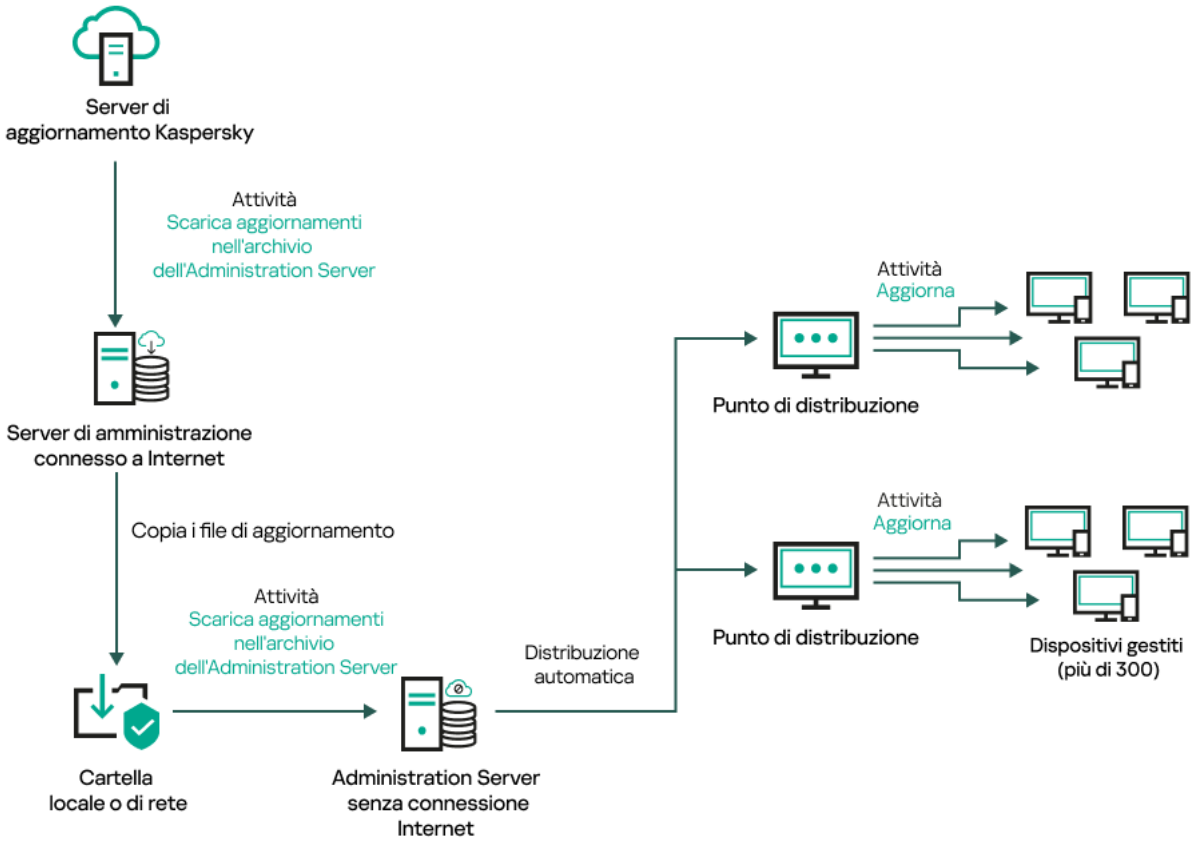
Tramite una cartella locale o di rete se Administration Server non dispone della connessione a Internet

Se Administration Server non dispone della connessione a Internet, è possibile configurare l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* per scaricare gli aggiornamenti da una cartella locale o di rete. In questo caso, di tanto in tanto è necessario copiare i file di aggiornamento necessari nella cartella specificata. È ad esempio possibile copiare i file di aggiornamento necessari da una delle seguenti origini:

- Administration Server con una connessione Internet (vedere la figura seguente)

  Poiché un Administration Server scarica solo gli aggiornamenti richiesti dalle applicazioni di protezione, i set di applicazioni di protezione gestiti dagli Administration Server (quello con una connessione Internet e quello senza connessione), devono corrispondere.

  Se l'Administration Server utilizzato per scaricare gli aggiornamenti dispone della versione 13.2 o precedente, aprire le proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, quindi abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**.



Aggiornamento tramite una cartella locale o di rete se Administration Server non dispone di una connessione Internet

- Kaspersky Update Utility

  Poiché questa utilità utilizza il vecchio schema per scaricare gli aggiornamenti, aprire le proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, quindi abilitare l'opzione *Scarica gli aggiornamenti utilizzando lo schema precedente*.

Creazione dell'attività Scarica aggiornamenti nell'archivio dell'Administration Server

L'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* consente di scaricare gli aggiornamenti dei database e dei moduli software per le applicazioni di protezione Kaspersky dai server degli aggiornamenti di Kaspersky all'archivio dell'Administration Server.

L'Avvio rapido guidato di Kaspersky Security Center crea automaticamente l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* dell'Administration Server. Nell'elenco delle attività, può esistere solo un'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. È possibile creare nuovamente questa attività se viene rimossa dall'elenco delle attività dell'Administration Server.

Dopo aver completato l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* e scaricato gli aggiornamenti, questi possono essere propagati ai dispositivi gestiti.

Prima di distribuire gli aggiornamenti ai dispositivi gestiti, è possibile eseguire l'attività di *verifica degli aggiornamenti*. Ciò consente di assicurarsi che l'Administration Server installi correttamente gli aggiornamenti scaricati e che il livello di sicurezza non diminuisca a causa degli aggiornamenti. Per verificarli prima della distribuzione, configurare l'opzione **Esegui la verifica degli aggiornamenti** nelle impostazioni dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*.

Per creare un'attività Scarica aggiornamenti nell'archivio dell'Administration Server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center, selezionare il tipo di attività **Scarica aggiornamenti nell'archivio dell'Administration Server**.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Nella pagina **Completa creazione attività** dell'attività, è possibile abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** per aprire la finestra delle proprietà dell'attività e modificare le impostazioni predefinite dell'attività. In caso contrario, è possibile configurare le impostazioni dell'attività in un secondo momento, quando desiderato.
6. Fare clic sul pulsante **Fine**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
7. Fare clic sul nome dell'attività creata per aprire la finestra delle relative proprietà.
8. Nella finestra delle proprietà visualizzata, nella scheda **Impostazioni applicazione**, specificare le seguenti impostazioni:

   - Sorgenti degli aggiornamenti

Come sorgente degli aggiornamenti, è possibile utilizzare i server di aggiornamento di Kaspersky, una cartella locale o di rete o un Administration Server primario.

Nell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* e nell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'autenticazione degli utenti non funziona se si seleziona una cartella locale o di rete protetta da password come origine degli aggiornamenti. Per risolvere questo problema, montare prima la cartella protetta da password, quindi specificare le credenziali richieste, ad esempio tramite il sistema operativo. Successivamente, è possibile selezionare questa cartella come origine degli aggiornamenti in un'attività di download degli aggiornamenti. Kaspersky Security Center Linux non richiede l'immissione delle credenziali.

- **Cartella per l'archiviazione degli aggiornamenti**

  Il percorso della cartella specificata per l'archiviazione degli aggiornamenti salvati. È possibile copiare il percorso della cartella specificata negli appunti. Non è possibile modificare il percorso di una cartella specificata per un'attività di gruppo.

- **Forza aggiornamento degli Administration Server secondari**

  Se questa opzione è abilitata, Administration Server avvia le attività di aggiornamento negli Administration Server secondari non appena vengono scaricati nuovi aggiornamenti. Le attività di aggiornamento vengono avviate utilizzando la sorgente dell'aggiornamento configurata nelle proprietà dell'attività negli Administration Server secondari.

  Se questa opzione è disabilitata, le attività di aggiornamento negli Administration Server secondari vengono avviate in base alla relativa pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Copia gli aggiornamenti scaricati in cartelle aggiuntive**

  Dopo avere ricevuto gli aggiornamenti, l'Administration Server li copia nelle cartelle specificate. Utilizzare questa opzione se si desidera gestire manualmente la distribuzione degli aggiornamenti nella rete.

  Questa opzione può ad esempio essere utilizzata nella seguente situazione: la rete dell'organizzazione è composta da diverse subnet indipendenti e i dispositivi in ciascuna subnet non hanno accesso ad altre subnet. I dispositivi in tutte le subnet hanno tuttavia accesso a una condivisione di rete comune. In questo caso, è possibile impostare Administration Server in una delle subnet per il download degli aggiornamenti dai server di aggiornamento Kaspersky, abilitare questa opzione e quindi specificare la condivisione di rete. Nelle attività di download degli aggiornamenti nell'archivio per gli altri Administration Server specificare la stessa condivisione di rete come sorgente degli aggiornamenti.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Scarica file diff**

  Questa opzione consente di abilitare la funzionalità di download dei file diff.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Scarica gli aggiornamenti utilizzando lo schema precedente**

A partire dalla versione 14, Kaspersky Security Center Linux scarica gli aggiornamenti dei database e dei moduli software utilizzando il nuovo schema. Affinché l'applicazione possa scaricare gli aggiornamenti utilizzando il nuovo schema, la sorgente degli aggiornamenti deve contenere i file di aggiornamento con i metadati compatibili con il nuovo schema. Se la sorgente degli aggiornamenti contiene i file di aggiornamento con i metadati compatibili solo con lo schema precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**. In caso contrario, l'attività di download degli aggiornamenti avrà esito negativo.

È ad esempio necessario abilitare questa opzione quando una cartella locale o di rete è specificata come sorgente degli aggiornamenti e i file di aggiornamento in questa cartella sono stati scaricati da una delle seguenti applicazioni:

- Kaspersky Update Utility

  Questa utilità scarica gli aggiornamenti utilizzando lo schema precedente.

- Guida di Kaspersky Security Center 13 Linux

  Ad esempio, Administration Server 1 non dispone di una connessione Internet. In questo caso, è possibile scaricare gli aggiornamenti utilizzando un Administration Server 2 dotato di una connessione Internet, quindi posizionare gli aggiornamenti in una cartella locale o di rete per utilizzarlo come sorgente degli aggiornamenti per Administration Server 1. Se Administration Server 2 dispone della versione 13, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente** nell'attività per Administration Server 1.

Per impostazione predefinita, questa opzione è disabilitata.

- **Esegui la verifica degli aggiornamenti**

  Administration Server esegue il download degli aggiornamenti dalla sorgente, li salva in un archivio temporaneo ed esegue l'attività definita nel campo **Attività di verifica degli aggiornamenti**. Se l'attività viene completata correttamente, gli aggiornamenti verranno copiati dall'archivio temporaneo in una cartella condivisa di Administration Server e saranno distribuiti in tutti gli altri dispositivi per cui Administration Server opera come sorgente degli aggiornamenti (verranno avviate le attività con il tipo di pianificazione **Quando vengono scaricati nuovi aggiornamenti nell'archivio**). L'attività di download degli aggiornamenti nell'archivio viene conclusa solo una volta completata l'attività *Verifica aggiornamenti*.

  Per impostazione predefinita, questa opzione è disabilitata.

9. Nella finestra delle proprietà dell'attività, nella scheda **Pianificazione**, creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

   - **Avvio pianificato**:

     - **Manualmente** (opzione selezionata per impostazione predefinita)

       L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

       Per impostazione predefinita, questa opzione è selezionata.

     - **Ogni N minuti**

       L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

       Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

- **Ogni N ore**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

  Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N giorni**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

  Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N settimane**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì all'ora di sistema corrente.

- **Giornaliera (ora legale non supportata)**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

  Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center Linux.

  Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

- **Settimanale**

  L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Ogni mese nei giorni specificati delle settimane selezionate**

L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è le 18:00.

- **Al completamento di un'altra attività**

  L'attività corrente viene avviata dopo il completamento di un'altra attività. È possibile selezionare la modalità di completamento dell'attività precedente (correttamente o con errori) per l'attivazione dell'avvio dell'attività corrente. Questo parametro funziona solo se entrambe le attività sono assegnate agli stessi dispositivi.

- Impostazioni aggiuntive dell'attività:

  - **Esegui attività non effettuate**

    Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

    Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

    Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Usa automaticamente il ritardo casuale per l'avvio delle attività**

    Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

    Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

    Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  - **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

    Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

    Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

    Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

  - **Arresta se l'attività viene eseguita per più di (min)**

Al termine del periodo di tempo specificato, l'attività viene arrestata automaticamente, che sia stata completata o meno.

Abilitare questa opzione se si desidera interrompere (o arrestare) le attività che richiedono troppo tempo per l'esecuzione.

Per impostazione predefinita, questa opzione è disabilitata. Il tempo predefinito per l'esecuzione dell'attività è 120 minuti.

10. Fare clic sul pulsante **Salva**.

L'attività verrà creata e configurata.

Quando Administration Server esegue l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, gli aggiornamenti dei database e dei moduli software vengono scaricati dalla sorgente degli aggiornamenti e archiviati nella cartella condivisa di Administration Server. Se questa attività viene creata per un gruppo di amministrazione, verrà applicata solo ai Network Agent inclusi nel gruppo di amministrazione specificato.

Gli aggiornamenti vengono distribuiti nei dispositivi client e negli Administration Server secondari dalla cartella condivisa di Administration Server.

Verifica degli aggiornamenti scaricati

Prima di installare gli aggiornamenti nei dispositivi gestiti, è possibile verificare la possibilità di utilizzare gli aggiornamenti e gli eventuali errori tramite l'attività *Verifica aggiornamenti*. L'attività di *verifica degli aggiornamenti* viene eseguita automaticamente nell'ambito dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. Administration Server scarica gli aggiornamenti dalla sorgente, li salva nell'archivio temporaneo ed esegue l'attività *Verifica aggiornamenti*. Se l'attività viene completata correttamente, gli aggiornamenti sono copiati dall'archivio temporaneo nella cartella condivisa di Administration Server. Vengono distribuiti a tutti i dispositivi client per cui l'Administration Server opera come sorgente degli aggiornamenti.

Se i risultati dell'attività *Verifica aggiornamenti* mostrano che gli aggiornamenti presenti nell'archivio temporaneo non sono corretti o se l'attività *Verifica aggiornamenti* viene completata con un errore, gli aggiornamenti non vengono copiati nella cartella condivisa. L'Administration Server mantiene il set di aggiornamenti precedente. Inoltre, le attività con il tipo di pianificazione **Quando vengono scaricati nuovi aggiornamenti nell'archivio** non vengono avviate. Tali operazioni vengono eseguite al successivo avvio dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, se la scansione dei nuovi aggiornamenti viene completata correttamente.

Un set di aggiornamenti è considerato non valido se viene soddisfatta una delle seguenti condizioni in almeno un dispositivo di test:

- Si è verificato un errore dell'attività di aggiornamento.
- Lo stato della protezione in tempo reale dell'applicazione di protezione è cambiato dopo l'applicazione degli aggiornamenti.
- È stato rilevato un oggetto infetto durante l'esecuzione dell'attività di scansione su richiesta.
- Si è verificato un errore di runtime di un'applicazione Kaspersky.

Se nei dispositivi di test non si verifica alcuna delle condizioni elencate, il set di aggiornamenti viene considerato valido e l'attività *Verifica aggiornamenti* viene considerata completata correttamente.

Prima di iniziare a creare l'attività *Verifica aggiornamenti*, eseguire i prerequisiti:

1. Creare un gruppo di amministrazione con diversi dispositivi di test. Sarà necessario questo gruppo per verificare gli aggiornamenti.

   È consigliabile utilizzare dispositivi con il livello di protezione più affidabile e con la configurazione delle applicazioni più diffusa nella rete. Questo approccio aumenta la qualità e la probabilità di rilevamento dei virus durante le scansioni e riduce al minimo il rischio di falsi positivi. Se vengono rilevati virus nei dispositivi di test, l'attività *Verifica aggiornamenti* viene considerata non riuscita.

2. Creare le attività di aggiornamento e scansione malware per un'applicazione supportata da Kaspersky Security Center Linux, ad esempio Kaspersky Endpoint Security for Linux. Quando si creano le attività di aggiornamento e scansione malware, specificare il gruppo di amministrazione con i dispositivi di test.

   L'attività *Verifica aggiornamenti* esegue in sequenza le attività di aggiornamento e scansione malware nei dispositivi di test per verificare che tutti gli aggiornamenti siano validi. Inoltre, durante la creazione dell'attività *Verifica aggiornamenti*, è necessario specificare le attività di aggiornamento e scansione malware.

3. Creare l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*.

Per fare in modo che Kaspersky Security Center Linux verifichi gli aggiornamenti scaricati prima di distribuirli ai dispositivi client:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sull'attività **Scarica aggiornamenti nell'archivio dell'Administration Server**.
3. Nella finestra delle proprietà dell'attività visualizzata, passare alla scheda **Impostazioni applicazione**, quindi abilitare l'opzione **Esegui la verifica degli aggiornamenti**.
4. Se l'attività di *verifica dell'aggiornamento* esiste, fare clic sul pulsante **Seleziona attività**. Nella finestra visualizzata selezionare l'attività *Verifica aggiornamenti* nel gruppo di amministrazione con dispositivi di test.
5. Se non è stata creata l'attività *Verifica aggiornamenti* in precedenza, procedere come segue:

   a. Fare clic sul pulsante **Nuova attività**.

   b. Nella Creazione guidata nuova attività visualizzata, specificare il nome dell'attività se si desidera modificare il nome preimpostato.

   c. Selezionare il gruppo di amministrazione con i dispositivi di test creato in precedenza.

   d. In primo luogo, selezionare l'attività di aggiornamento di un'applicazione desiderata supportata da Kaspersky Security Center Linux, quindi selezionare l'attività di scansione malware.

   Successivamente, vengono visualizzate le seguenti opzioni. È consigliabile lasciarle abilitate:

   - **Riavvia il dispositivo dopo l'aggiornamento del database**

     Dopo l'aggiornamento dei database anti-virus in un dispositivo, è consigliabile riavviare il dispositivo.

     Per impostazione predefinita, l'opzione è abilitata.

   - **Verifica lo stato della protezione in tempo reale dopo l'aggiornamento del database e il riavvio del dispositivo**

Se questa opzione è abilitata, l'attività *Verifica aggiornamenti* verifica se gli aggiornamenti scaricati nell'archivio dell'Administration Server sono validi e se il livello di protezione è diminuito dopo l'aggiornamento dei database anti-virus e il riavvio del dispositivo.

Per impostazione predefinita, questa opzione è abilitata.

e. Specificare un account da cui verrà eseguita l'attività *Verifica aggiornamenti*. È possibile utilizzare il proprio account e lasciare abilitata l'opzione **Account predefinito**. In alternativa, è possibile specificare che l'attività deve essere eseguita con un altro account che disponga dei diritti di accesso necessari. A tale scopo, selezionare l'opzione **Specifica account**, quindi immettere le credenziali di tale account.

6. Fare clic su **Salva** per chiudere la finestra delle proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*.

La verifica automatica degli aggiornamenti è abilitata. Adesso è possibile eseguire l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, che inizierà dalla verifica degli aggiornamenti.

Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione

È possibile creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per un gruppo di amministrazione. L'attività verrà eseguita per i punti di distribuzione inclusi nel gruppo di amministrazione specificato.

È ad esempio possibile utilizzare questa attività se il costo del traffico tra l'Administration Server e i punti di distribuzione è superiore rispetto a quello del traffico tra i punti di distribuzione e i server di aggiornamento Kaspersky oppure se l'Administration Server non dispone di accesso a Internet.

Questa attività è necessaria per scaricare gli aggiornamenti dai server di aggiornamento Kaspersky negli archivi dei punti di distribuzione. L'elenco degli aggiornamenti include:

- Aggiornamenti dei database e dei moduli software delle applicazioni di protezione Kaspersky
- Aggiornamenti dei componenti di Kaspersky Security Center
- Aggiornamenti delle applicazioni di protezione Kaspersky

Dopo aver scaricato gli aggiornamenti, questi possono essere propagati ai dispositivi gestiti.

*Per creare l'attività **Scarica aggiornamenti negli archivi dei punti di distribuzione** per un gruppo di amministrazione selezionato:*

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center, nel campo **Tipo di attività** selezionare **Scarica aggiornamenti negli archivi dei punti di distribuzione**.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

5. Selezionare un pulsante di opzione per specificare il gruppo di amministrazione, la selezione dispositivi o i dispositivi a cui si applica l'attività.

6. Nel passaggio **Completa creazione attività** dell'attività, se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

7. Fare clic sul pulsante **Crea**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.

8. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

9. Nella scheda **Impostazioni applicazione** della finestra delle proprietà dell'attività specificare le seguenti impostazioni:

   - **Sorgenti degli aggiornamenti**

     È possibile utilizzare le seguenti risorse come sorgenti degli aggiornamenti per il punto di distribuzione:

     - Server degli aggiornamenti Kaspersky

       I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.

       Questa opzione è selezionata per impostazione predefinita.

     - Administration Server primario

       Questa risorsa si applica alle attività create per un Administration Server secondario o virtuale.

     - Cartella locale o di rete

       Un'unità locale o una cartella di rete che contiene gli aggiornamenti più recenti. Solo una condivisione SMB montata può essere utilizzata come cartella di rete. Quando si seleziona una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server.

       Nell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* e nell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'autenticazione degli utenti non funziona se si seleziona una cartella locale o di rete protetta da password come origine degli aggiornamenti. Per risolvere questo problema, montare prima la cartella protetta da password, quindi specificare le credenziali richieste, ad esempio tramite il sistema operativo. Successivamente, è possibile selezionare questa cartella come origine degli aggiornamenti in un'attività di download degli aggiornamenti. Kaspersky Security Center Linux non richiede l'immissione delle credenziali.

   - **Cartella per l'archiviazione degli aggiornamenti**

     Il percorso della cartella specificata per l'archiviazione degli aggiornamenti salvati. È possibile copiare il percorso della cartella specificata negli appunti. Non è possibile modificare il percorso di una cartella specificata per un'attività di gruppo.

   - **Scarica file diff**

Questa opzione consente di abilitare la funzionalità di download dei file diff.

Per impostazione predefinita, questa opzione è disabilitata.

- **Scarica gli aggiornamenti utilizzando lo schema precedente**

  A partire dalla versione 14, Kaspersky Security Center Linux scarica gli aggiornamenti dei database e dei moduli software utilizzando il nuovo schema. Affinché l'applicazione possa scaricare gli aggiornamenti utilizzando il nuovo schema, la sorgente degli aggiornamenti deve contenere i file di aggiornamento con i metadati compatibili con il nuovo schema. Se la sorgente degli aggiornamenti contiene i file di aggiornamento con i metadati compatibili solo con lo schema precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**. In caso contrario, l'attività di download degli aggiornamenti avrà esito negativo.

  È ad esempio necessario abilitare questa opzione quando una cartella locale o di rete è specificata come sorgente degli aggiornamenti e i file di aggiornamento in questa cartella sono stati scaricati da una delle seguenti applicazioni:

  - Kaspersky Update Utility

    Questa utilità scarica gli aggiornamenti utilizzando lo schema precedente.

  - Guida di Kaspersky Security Center 13 Linux

    Un punto di distribuzione è ad esempio configurato per acquisire gli aggiornamenti da una cartella locale o di rete. In questo caso, è possibile scaricare gli aggiornamenti utilizzando un Administration Server dotato di una connessione Internet, quindi posizionare gli aggiornamenti nella cartella locale nel punto di distribuzione. Se la versione di Administration Server è la 13, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente** nell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

  Per impostazione predefinita, questa opzione è disabilitata.

10. Creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato**:

  - **Manualmente** (opzione selezionata per impostazione predefinita)

    L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Ogni N ore**

L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N giorni**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

  Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N settimane**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì all'ora di sistema corrente.

- **Giornaliera (ora legale non supportata)**

  L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

  Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center Linux.

  Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

- **Settimanale**

  L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Ogni mese nei giorni specificati delle settimane selezionate**

L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è le 18:00.

- **Durante un'epidemia di virus**

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

  L'attività corrente viene avviata dopo il completamento di un'altra attività. È possibile selezionare la modalità di completamento dell'attività precedente (correttamente o con errori) per l'attivazione dell'avvio dell'attività corrente. Questo parametro funziona solo se entrambe le attività sono assegnate agli stessi dispositivi.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

11. Fare clic sul pulsante **Salva**.

    L'attività verrà creata e configurata.

    Oltre alle impostazioni specificate durante la creazione dell'attività, è possibile modificare altre proprietà di un'attività creata.

Quando si esegue l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, gli aggiornamenti dei database e dei moduli software vengono scaricati dalla sorgente degli aggiornamenti e archiviati nella cartella condivisa. Gli aggiornamenti scaricati verranno utilizzati solo dai punti di distribuzione inclusi nel gruppo di amministrazione specificato e che non hanno alcuna attività di download degli aggiornamenti esplicitamente configurata.

Aggiunta di sorgenti degli aggiornamenti per l'attività Scarica aggiornamenti nell'archivio di Administration Server

Quando si crea o utilizza l'attività per il download degli aggiornamenti nell'archivio di Administration Server, è possibile scegliere le seguenti sorgente degli aggiornamenti:

- Server degli aggiornamenti Kaspersky
- Administration Server primario

  Questa risorsa si applica alle attività create per un Administration Server secondario o virtuale.
- Cartella locale o di rete

Nell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* e nell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'autenticazione degli utenti non funziona se si seleziona una cartella locale o di rete protetta da password come origine degli aggiornamenti. Per risolvere questo problema, montare prima la cartella protetta da password, quindi specificare le credenziali richieste, ad esempio tramite il sistema operativo. Successivamente, è possibile selezionare questa cartella come origine degli aggiornamenti in un'attività di download degli aggiornamenti. Kaspersky Security Center Linux non richiede l'immissione delle credenziali.

I server di aggiornamento Kaspersky vengono utilizzati per impostazione predefinita, ma è possibile scaricare gli aggiornamenti anche da una cartella locale o di rete. È possibile che si desideri utilizzare la cartella se la rete non dispone di accesso a Internet. In questo caso, è possibile scaricare manualmente gli aggiornamenti dai server di aggiornamento Kaspersky e inserire i file scaricati nella cartella necessaria.

È possibile specificare un solo percorso per una cartella locale o di rete. Come cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server. Come cartella di rete, è possibile utilizzare un server FTP o HTTP o una condivisione SMB. Se una condivisione SMB richiede l'autenticazione, deve essere montata anticipatamente nel sistema con le credenziali richieste. Si consiglia di non utilizzare il protocollo SMB1 poiché non è sicuro.

Se si aggiungono sia i server degli aggiornamenti Kaspersky sia la cartella locale o di rete, gli aggiornamenti verranno scaricati prima dalla cartella. In caso di errore durante il download, verranno utilizzati i server di aggiornamento Kaspersky.

Per aggiungere le sorgenti degli aggiornamenti:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Scarica aggiornamenti nell'archivio dell'Administration Server**.
3. Passare alla scheda **Impostazioni applicazione**.
4. Nella riga **Sorgenti degli aggiornamenti**, fare clic sul pulsante **Configura**.
5. Nella finestra visualizzata fare clic sul pulsante **Aggiungi**.
6. Nell'elenco delle sorgenti degli aggiornamenti, aggiungere le sorgenti necessarie. Se si seleziona la casella di controllo **Cartella locale o di rete**, specificare un percorso per la cartella.
7. Fare clic su **OK**, quindi chiudere la finestra delle proprietà della sorgente degli aggiornamenti.
8. Nella finestra della sorgente degli aggiornamenti, fare clic su **OK**.
9. Fare clic sul pulsante **Salva** nella finestra dell'attività.

A questo punto, gli aggiornamenti vengono scaricati nell'archivio di Administration Server dalle origini specificate.

Installazione automatica degli aggiornamenti per Kaspersky Endpoint Security for Windows

È possibile configurare gli aggiornamenti automatici dei database e dei moduli software di Kaspersky Endpoint Security for Windows nei dispositivi client.

Per configurare il download e l'installazione automatica degli aggiornamenti di Kaspersky Endpoint Security for Windows nei dispositivi:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Endpoint Security for Windows, selezionare **Aggiornamento** come sottotipo di attività.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Scegliere l'ambito dell'attività.
6. Specificare il gruppo di amministrazione, la selezione dispositivi o i dispositivi a cui si applica l'attività.
7. Nel passaggio **Completa creazione attività** dell'attività, se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
8. Fare clic sul pulsante **Crea**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
9. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.
10. Nella scheda **Impostazioni applicazione** della finestra delle proprietà dell'attività definire le impostazioni dell'attività di aggiornamento in modalità locale o mobile:

    - **Modalità locale**: Viene stabilita la connessione tra il dispositivo e Administration Server.
    - **Modalità mobile**: non viene stabilita alcuna connessione tra Kaspersky Security Center Linux e il dispositivo (ad esempio quando il dispositivo non è connesso a Internet).
11. Abilitare le sorgenti degli aggiornamenti che si desidera utilizzare per aggiornare i database e i moduli dell'applicazione per Kaspersky Endpoint Security for Windows. Se necessario, modificare le posizioni delle sorgenti nell'elenco utilizzando i pulsanti **Sposta su** e **Sposta giù**. Se sono abilitate diverse sorgenti degli aggiornamenti, Kaspersky Endpoint Security for Windows tenta di connettersi a tali sorgenti una dopo l'altra, a partire a quella all'inizio dell'elenco, ed esegue l'attività di aggiornamento recuperando il pacchetto di aggiornamento dalla prima sorgente disponibile.
12. Abilitare l'opzione **Installa gli aggiornamenti approvati del modulo delle applicazioni** per scaricare e installare gli aggiornamenti dei moduli software oltre ai database dell'applicazione.

    Se l'opzione è abilitata, Kaspersky Endpoint Security for Windows invia una notifica all'utente per informarlo degli aggiornamenti dei moduli software disponibili e include gli aggiornamenti dei moduli software nel pacchetto di aggiornamento durante l'esecuzione dell'attività di aggiornamento. Kaspersky Endpoint Security for Windows installa solo gli aggiornamenti per cui è stato impostato lo stato *Approvato*. Verranno installati in locale tramite l'interfaccia dell'applicazione o tramite Kaspersky Security Center Linux.

    È inoltre possibile abilitare l'opzione **Installa automaticamente gli aggiornamenti critici del modulo delle applicazioni**. Se sono disponibili aggiornamenti per i moduli software, Kaspersky Endpoint Security for Windows li installa automaticamente con lo stato *Critico*. Gli aggiornamenti rimanenti saranno installati dopo essere stati approvati dall'amministratore.

Se l'aggiornamento dei moduli software richiede la visualizzazione e l'accettazione delle condizioni del Contratto di licenza e dell'Informativa sulla privacy, l'applicazione installa gli aggiornamenti dopo che le condizioni del Contratto di licenza e dell'Informativa sulla privacy sono state accettate dall'utente.

13. Selezionare la casella di controllo **Copia aggiornamenti nella cartella** per fare in modo che gli aggiornamenti scaricati vengano salvati in una cartella, quindi specificare il percorso della cartella.

14. Pianificare l'attività. Per garantire aggiornamenti tempestivi, è consigliabile selezionare l'opzione **Quando vengono scaricati nuovi aggiornamenti nell'archivio**.

15. Fare clic su **Salva**.

Quando è in esecuzione l'attività **Aggiornamento**, l'applicazione invia richieste ai server di aggiornamento Kaspersky.

Alcuni aggiornamenti richiedono l'installazione delle versioni più recenti dei plug-in di gestione.

Informazioni sull'utilizzo dei file diff per l'aggiornamento dei database e dei moduli del software Kaspersky

Quando Kaspersky Security Center Linux scarica gli aggiornamenti dai server di aggiornamento Kaspersky, ottimizza il traffico utilizzando file diff. È anche possibile abilitare l'utilizzo dei file diff da parte dei dispositivi (Administration Server, punti di distribuzione e dispositivi client) che recuperano gli aggiornamenti da altri dispositivi della rete.

Informazioni sulla funzionalità Download dei file diff

Un file diff descrive le differenze tra due versioni di un file di un database o un modulo software. L'utilizzo dei file diff riduce il traffico all'interno della rete aziendale, poiché i file diff occupano meno spazio rispetto ai file completi di database e moduli software. Se è abilitata la funzionalità *Download dei file diff* in un Administration Server o un punto di distribuzione, i file diff vengono salvati in questo Administration Server o punto di distribuzione. Come risultato, i dispositivi che recuperano gli aggiornamenti da questo Administration Server o punto di distribuzione possono utilizzare i file diff salvati per l'aggiornamento dei database e dei moduli software.

Per ottimizzare l'utilizzo dei file diff, è consigliabile sincronizzare la pianificazione di aggiornamento dei dispositivi con la pianificazione di aggiornamento dell'Administration Server o del punto di distribuzione da cui i dispositivi recuperano gli aggiornamenti. Il traffico può comunque essere ridotto anche se i dispositivi vengono aggiornati con una frequenza notevolmente inferiore a quella dell'Administration Server o del punto di distribuzione da cui i dispositivi recuperano gli aggiornamenti.

I punti di distribuzione non utilizzano la modalità IP multicast per la distribuzione automatica dei file diff.

Abilitazione della funzionalità Download dei file diff

Passaggi

1. **Abilitazione della funzionalità in Administration Server**

   Abilitare la funzionalità nelle *impostazioni di un'attività Scarica aggiornamenti nell'archivio dell'Administration Server*.

2. **Abilitazione della funzionalità per un punto di distribuzione**

   Abilitare la funzionalità per un punto di distribuzione che riceve gli aggiornamenti tramite un'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

   Successivamente, abilitare la funzionalità nelle impostazioni del criterio di Network Agent per un punto di distribuzione che riceve gli aggiornamenti da Administration Server.

   Successivamente abilitare la funzionalità per un punto di distribuzione che riceve gli aggiornamenti da Administration Server.

   La funzionalità è abilitata nelle impostazioni del criterio di Network Agent e, se sono stati assegnati manualmente punti di distribuzione e se si desidera sostituire le impostazioni del criterio, nella **sezione Punti di distribuzione**.

Per verificare che la funzionalità Download dei file diff sia abilitata correttamente, è possibile misurare il traffico interno prima e dopo l'esecuzione dello scenario.

Download degli aggiornamenti tramite punti di distribuzione

Kaspersky Security Center Linux consente ai punti di distribuzione di ricevere aggiornamenti dall'Administration Server, dai server di Kaspersky o da una cartella locale o di rete.

Per configurare il download degli aggiornamenti per un punto di distribuzione:

1. Nel menu principale, fare clic sull'icona delle impostazioni (⚙) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Fare clic sul nome del punto di distribuzione attraverso il quale verranno distribuiti gli aggiornamenti ai dispositivi client nel gruppo.

4. Nella finestra delle proprietà del punto di distribuzione selezionare la sezione **Sorgente degli aggiornamenti**.

5. Selezionare una sorgente degli aggiornamenti per il punto di distribuzione:

   - **Sorgente degli aggiornamenti**

Selezionare una sorgente degli aggiornamenti per il punto di distribuzione:

- Per consentire al punto di distribuzione di ricevere gli aggiornamenti da Administration Server, selezionare **Recupera da Administration Server**:
- Per consentire al punto di distribuzione di ricevere gli aggiornamenti tramite un'attività, selezionare **Usa l'attività di download degli aggiornamenti**, quindi specificare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*:
  - Se tale attività esiste già nel dispositivo, selezionare l'attività nell'elenco.
  - Se tale attività non esiste ancora nel dispositivo, fare clic sul collegamento **Crea attività** per creare un'attività. Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

- **Scarica file diff**

  Questa opzione consente di abilitare la funzionalità di download dei file diff.

  Per impostazione predefinita, questa opzione è abilitata.

Il punto di distribuzione riceverà gli aggiornamenti dalla sorgente specificata.

Aggiornamento dei database e dei moduli software Kaspersky nei dispositivi offline

L'aggiornamento dei database e dei moduli software Kaspersky nei dispositivi gestiti è un'attività importante per mantenere la protezione dei dispositivi da virus e altre minacce. Gli amministratori in genere configurano aggiornamenti periodici tramite l'archivio di Administration Server.

Quando è necessario aggiornare i database e i moduli software in un dispositivo (o un gruppo di dispositivi) che non è connesso all'Administration Server (primario o secondario), a un punto di distribuzione o a Internet, è necessario utilizzare sorgenti degli aggiornamenti alternative, come un server FTP o una cartella locale. In questo caso, è necessario distribuire i file degli aggiornamenti richiesti utilizzando un dispositivo di archiviazione di massa, come un'unità flash o un disco rigido esterno.

È possibile copiare gli aggiornamenti richiesti da:

- Administration Server.

  Per essere certi che l'archivio dell'Administration Server contenga gli aggiornamenti richiesti per l'applicazione di protezione installata in un dispositivo offline, in almeno uno dei dispositivi online gestiti deve essere installata la stessa applicazione di protezione. Questa applicazione deve essere configurata per ricevere gli aggiornamenti dall'archivio di Administration Server tramite l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*.

- Qualsiasi dispositivo in cui sia installata e configurata la stessa applicazione di protezione per la ricezione degli aggiornamenti dall'archivio dell'Administration Server, dall'archivio di un punto di distribuzione o direttamente dai server di aggiornamento Kaspersky.

Di seguito è riportato un esempio di configurazione degli aggiornamenti dei database e dei moduli software copiandoli dall'archivio di Administration Server.

Per aggiornare i database e i moduli software Kaspersky nei dispositivi offline:

1. Connettere l'unità rimovibile al dispositivo in cui è installato Administration Server.
2. Copiare i file degli aggiornamenti nell'unità rimovibile.

   Per impostazione predefinita, gli aggiornamenti si trovano in: /var/opt/kaspersky/klnagent_srv/1093/.working/share_srv/Updates/.

   In alternativa, è possibile configurare Kaspersky Security Center Linux per copiare periodicamente gli aggiornamenti nella cartella selezionata. A tale scopo, utilizzare l'opzione **Copia gli aggiornamenti scaricati in cartelle aggiuntive** nelle proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. Se si specifica una cartella posizionata in un'unità flash o un disco rigido esterno come cartella di destinazione per questa opzione, tale dispositivo di archiviazione di massa conterrà sempre la versione più recente degli aggiornamenti.
3. Nei dispositivi offline configurare Kaspersky Endpoint Security) per la ricezione degli aggiornamenti da una cartella locale o una risorsa condivisa, come un server FTP o una cartella condivisa.

   Istruzioni dettagliate:

   - Guida di Kaspersky Endpoint Security for Linux
   - Guida di Kaspersky Endpoint Security for Windows
4. Copiare i file degli aggiornamenti dall'unità rimovibile nella cartella locale o nella risorsa condivisa che si desidera utilizzare come sorgente degli aggiornamenti.
5. Nel dispositivo offline che richiede l'installazione degli aggiornamenti, avviare l'attività di *aggiornamento* di Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security for Windows, a seconda del sistema operativo del dispositivo offline.

Al termine dell'attività di aggiornamento, i database e i moduli software Kaspersky sono aggiornati nel dispositivo.

Backup e ripristino dei plug-in Web

Kaspersky Security Center Web Console consente di eseguire il backup dello stato corrente di un plug-in Web per poter ripristinare lo stato salvato in un secondo momento. È ad esempio possibile eseguire il backup di un plug-in Web prima di eseguirne l'aggiornamento a una versione più recente. Dopo l'aggiornamento, se la versione più recente non soddisfa i requisiti o le aspettative dell'utente, è possibile ripristinare la versione precedente del plug-in Web dal backup.

Per eseguire il backup dei plug-in Web:

1. Nel menu principale accedere a **Impostazioni** → **Plug-in Web**.
2. Nella sezione **Plug-in Web** selezionare i plug-in Web di cui si desidera eseguire il backup, quindi fare clic sul pulsante **Crea copia di backup**.

Viene eseguito il backup dei plug-in Web selezionati. È possibile visualizzare i backup creati nella sezione **Backup**.

Per ripristinare un plug-in Web da un backup:

1. Nel menu principale, passare a **Impostazioni** → **Backup**.

2. Nella sezione **Backup** selezionare il backup del plug-in Web che si desidera ripristinare, quindi fare clic sul pulsante **Ripristina da backup**.

Il plug-in Web viene ripristinato dal backup selezionato.

Monitoraggio, generazione di rapporti e audit

Questa sezione illustra le funzionalità di monitoraggio e generazione dei rapporti di Kaspersky Security Center Linux. Queste funzionalità offrono una panoramica dell'infrastruttura, degli stati di protezione e delle statistiche.

Dopo la distribuzione di Kaspersky Security Center Linux o durante l'esecuzione, è possibile configurare le funzionalità di monitoraggio e generazione dei rapporti in base alle esigenze.

Scenario: monitoraggio e generazione dei rapporti

Questa sezione fornisce uno scenario per la configurazione della funzionalità di monitoraggio e generazione dei rapporti in Kaspersky Security Center Linux.

Prerequisiti

Dopo aver distribuito Kaspersky Security Center Linux nella rete di un'organizzazione, è possibile iniziare a monitorarlo e generare rapporti sul relativo funzionamento.

Il monitoraggio e la generazione dei rapporti nella rete di un'organizzazione prevede diversi passaggi:

1. **Configurazione del passaggio degli stati del dispositivo**

   Acquisire familiarità con le impostazioni per gli stati del dispositivo in base a condizioni specifiche. Modificando queste impostazioni, è possibile modificare il numero di eventi con livelli di importanza *Critico* o *Avviso*. Durante la configurazione del passaggio degli stati del dispositivo, verificare quanto segue:

   - Le nuove impostazioni non sono in conflitto con i criteri di sicurezza delle informazioni dell'organizzazione.
   - Si è in grado di reagire tempestivamente agli eventi di sicurezza importanti nella rete dell'organizzazione.

2. **Configurazione delle notifiche degli eventi nei dispositivi client**

   Istruzioni dettagliate:

   Configurare la notifica (tramite e-mail, SMS o avviando un file eseguibile) degli eventi nei dispositivi client

3. **Esecuzione delle azioni consigliate per le notifiche critiche e di avviso**

   Istruzioni dettagliate:

   Eseguire le azioni consigliate per la rete dell'organizzazione

4. **Analisi dello stato di sicurezza della rete dell'organizzazione**

   Istruzioni dettagliate:

   - Esaminare il widget Stato protezione
   - Generare ed esaminare il Rapporto sullo stato della protezione
   - Generare ed esaminare il Rapporto sugli errori

5. **Individuazione dei dispositivi client che non sono protetti**

   Istruzioni dettagliate:

   - Esaminare il widget Nuovi dispositivi

- Generare ed esaminare il Rapporto sulla distribuzione della protezione

6. **Verifica della protezione dei dispositivi client**

   Istruzioni dettagliate:

   - Generare ed esaminare i rapporti delle categorie Stato protezione e Statistiche delle minacce
   - Avviare ed esaminare la selezione eventi Critico

7. **Valutazione e limitazione del carico di eventi nel database**

   Le informazioni sugli eventi che si verificano durante il funzionamento delle applicazioni gestite vengono trasferite da un dispositivo client e registrate nel database di Administration Server. Per ridurre il carico su Administration Server, valutare e limitare il numero massimo di eventi che possono essere archiviati nel database.

   Istruzioni dettagliate:

   - Limitazione del numero massimo di eventi

8. **Analisi delle informazioni sulla licenza**

   Istruzioni dettagliate:

   - Aggiungere il widget Utilizzo chiavi di licenza al dashboard ed esaminarlo
   - Generare ed esaminare il Rapporto sull'utilizzo delle chiavi di licenza

Risultati

Al termine dello scenario, si dispone di informazioni sulla protezione della rete dell'organizzazione e quindi è possibile pianificare le azioni per il miglioramento della protezione.

Informazioni sui tipi di monitoraggio e generazione dei rapporti

Le informazioni sugli eventi di sicurezza nella rete di un'organizzazione sono archiviate nel database di Administration Server. In base agli eventi, Kaspersky Security Center Web Console fornisce i seguenti tipi di monitoraggio e generazione dei rapporti nella rete dell'organizzazione:

- Dashboard
- Rapporti
- Selezioni eventi
- Notifiche

Dashboard

Il dashboard consente di monitorare le tendenze relative alla sicurezza nella rete dell'organizzazione fornendo una visualizzazione grafica delle informazioni.

Rapporti

La funzionalità Rapporti consente di ottenere informazioni numeriche dettagliate sulla sicurezza della rete dell'organizzazione, nonché di salvare le informazioni in un file, inviarlo tramite e-mail e stamparlo.

Selezioni eventi

Le selezioni eventi consentono di visualizzare i set denominati degli eventi selezionati dal database di Administration Server. Questi set di eventi sono raggruppati in base alle seguenti categorie:

- In base al livello di importanza: **Eventi critici**, **Errori funzionali**, **Avvisi** e **Eventi informativi**
- In base al tempo: **Eventi recenti**
- In base al tipo: **Richieste utente** e **Eventi di controllo**

È possibile creare e visualizzare le selezioni eventi definite dall'utente in base alle impostazioni disponibili per la configurazione nell'interfaccia di Kaspersky Security Center Web Console.

Notifiche

Le notifiche segnalano gli eventi e consentono di velocizzare le risposte a tali eventi eseguendo le azioni consigliate o le azioni che si ritengono appropriate.

Dashboard e widget

Questa sezione contiene informazioni sul dashboard e sui widget forniti dal dashboard. La sezione include istruzioni su come gestire i widget e configurare le impostazioni dei widget.

Utilizzo del dashboard

Il dashboard consente di monitorare le tendenze relative alla sicurezza nella rete dell'organizzazione fornendo una visualizzazione grafica delle informazioni.

Il dashboard è disponibile in Kaspersky Security Center Web Console, nella sezione **Monitoraggio e generazione dei rapporti**, facendo clic su **Dashboard**.

Il dashboard fornisce widget che possono essere personalizzati. È possibile scegliere tra numerosi widget diversi, presentati come grafici a torta o grafici ad anello, tabelle, grafici, grafici a barre ed elenchi. Le informazioni visualizzate nei widget vengono aggiornate automaticamente, il periodo di aggiornamento è di uno o due minuti. L'intervallo tra gli aggiornamenti varia per i diversi widget. È possibile aggiornare manualmente i dati in un widget in qualsiasi momento tramite il menu delle impostazioni.

Per impostazione predefinita, i widget includono informazioni su tutti gli eventi archiviati nel database di Administration Server.

Kaspersky Security Center Web Console dispone di un set predefinito di widget per le seguenti categorie:

- **Stato protezione**
- **Distribuzione**
- **Aggiornamento**

- **Statistiche delle minacce**
- **Altro**

Alcuni widget contengono informazioni di testo con collegamenti. È possibile visualizzare informazioni dettagliate facendo clic su un collegamento.

Quando si configura il dashboard, è possibile aggiungere i widget desiderati, nascondere i widget non necessari, modificare le dimensioni o l'aspetto dei widget, spostare i widget e modificarne le impostazioni.

Aggiunta di widget al dashboard

Per aggiungere widget al dashboard:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sul pulsante **Aggiungi o ripristina widget Web**.
3. Nell'elenco dei widget disponibili selezionare i widget che si desidera aggiungere al dashboard.

   I widget sono raggruppati per categoria. Per visualizzare l'elenco dei widget inclusi in una categoria, fare clic sull'icona della freccia di espansione (>) accanto al nome della categoria.
4. Fare clic sul pulsante **Aggiungi**.

I widget selezionati verranno aggiunti alla fine del dashboard.

Ora è possibile modificare la rappresentazione e i parametri dei widget aggiunti.

Occultamento di un widget dal dashboard

Per nascondere un widget visualizzato dal dashboard:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera nascondere.
3. Selezionare **Nascondi widget Web**.
4. Nella finestra **Avviso** visualizzata fare clic su **OK**.

Il widget selezionato verrà nascosto. In seguito, è possibile aggiungere nuovamente il widget al dashboard.

Spostamento di un widget nel dashboard

Per spostare un widget nel dashboard:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera spostare.
3. Selezionare **Sposta**.
4. Fare clic sul punto in cui si desidera spostare il widget. È possibile selezionare solo un altro widget.

Le posizioni dei widget selezionati vengono scambiate.

Modifica delle dimensioni o dell'aspetto del widget

Per i widget che visualizzano un grafico, è possibile modificarne la rappresentazione: un grafico a barre o un grafico a linee. Per alcuni widget è possibile modificare le dimensioni: Compatto, Medio o Massimo.

Per modificare la rappresentazione del widget:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera modificare.
3. Eseguire una delle seguenti operazioni:
   - Per visualizzare il widget come grafico a barre, selezionare **Tipo di grafico: barre**.
   - Per visualizzare il widget come grafico a linee, selezionare **Tipo di grafico: linee**.
   - Per modificare l'area occupata dal widget, selezionare uno dei valori:
     - **Compatto**
     - **Compatto (solo barra)**
     - **Medio (grafico ad anello)**
     - **Medio (grafico a barre)**
     - **Massimo**

La rappresentazione del widget selezionato verrà modificata.

Modifica delle impostazioni del widget

Per modificare le impostazioni di un widget:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera modificare.
3. Selezionare **Mostra impostazioni**.

4. Nella finestra delle impostazioni del widget visualizzata modificare le impostazioni del widget come richiesto.

5. Fare clic su **Salva** per salvare le modifiche.

Le impostazioni del widget selezionato verranno modificate.

Il set di impostazioni dipende dallo specifico widget. Di seguito sono riportate alcune delle impostazioni comuni:

- **Ambito del widget Web** (il set di oggetti per cui il widget visualizza informazioni), ad esempio un gruppo di amministrazione o una selezione dispositivi.
- **Seleziona attività** (l'attività per cui il widget visualizza informazioni).
- **Intervallo** (l'intervallo di tempo per cui le informazioni vengono visualizzate nel widget): tra le due date specificate, dalla data specificata al giorno corrente o dal giorno corrente meno il numero di giorni specificato al giorno corrente.
- **Imposta su Critico se è specificato** e **Imposta su Avviso se è specificato** (le regole che determinano il colore di un indicatore a semaforo).

Dopo aver modificato le impostazioni del widget, è possibile aggiornare manualmente i dati nel widget.

Per aggiornare i dati su un widget:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera spostare.
3. Selezionare **Aggiorna**.

I dati nel widget vengono aggiornati.

Informazioni sulla modalità Solo dashboard

È possibile configurare la modalità Solo dashboard per i dipendenti che non gestiscono la rete ma che desiderano visualizzare le statistiche di protezione della rete in Kaspersky Security Center Linux (ad esempio un Top Manager). Con questa modalità abilitata, l'utente visualizza solo un dashboard con un set predefinito di widget. L'utente può quindi monitorare le statistiche specificate nei widget, ad esempio lo stato della protezione di tutti i dispositivi gestiti, il numero di minacce rilevate di recente o l'elenco delle minacce più frequenti nella rete.

Quando un utente usa la modalità Solo dashboard, vengono applicate le seguenti restrizioni:

- Il menu principale non viene mostrato all'utente, che non potrà quindi modificare le impostazioni di protezione della rete.
- L'utente non può eseguire alcuna azione con i widget, ad esempio aggiungerli o nasconderli. È pertanto necessario inserire tutti i widget necessari per l'utente nel dashboard e configurarli, ad esempio impostando la regola di conteggio degli oggetti o specificando l'intervallo di tempo.

Non è possibile assegnare a se stessi la modalità Solo dashboard. Se si desidera utilizzare questa modalità, contattare un amministratore di sistema, un MSP (Managed Service Provider) o un utente con il diritto **Modifica elenchi di controllo degli accessi agli oggetti** nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

Configurazione della modalità Solo dashboard

Prima di iniziare a configurare la modalità Solo dashboard, assicurarsi che vengano soddisfatti i seguenti prerequisiti:

- L'utente dispone del diritto **Modifica elenchi di controllo degli accessi agli oggetti** nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**. Se non si dispone di questo diritto, la scheda per la configurazione della modalità non sarà presente.
- L'utente ha il diritto **Lettura** nell'area funzionale **Caratteristiche generali: Funzionalità di base**.

Se nella rete è organizzata una gerarchia di Administration Server, per configurare la modalità Solo dashboard passare al Server in cui è disponibile l'account utente nella sezione **Utenti** tab of the **Utenti e ruoli** → **Utenti e gruppi**. Può trattarsi di un server primario o di un server secondario fisico. Non è possibile regolare la modalità in un server virtuale.

Per configurare la modalità Solo dashboard:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic sul nome dell'account utente per il quale si desidera modificare il dashboard con i widget.
3. Nella finestra delle impostazioni dell'account visualizzata selezionare la scheda **Dashboard**.

   Nella scheda aperta viene visualizzato lo stesso dashboard dell'utente.
4. Se l'opzione **Visualizza la console in modalità Solo dashboard** è abilitata, spostare l'interruttore per disabilitarla.

   Quando questa opzione è abilitata, non è nemmeno possibile modificare il dashboard. Dopo aver disabilitato l'opzione, è possibile gestire i widget.
5. Configurare l'aspetto del dashboard. Il set di widget preparato nella scheda **Dashboard** è disponibile per l'utente con l'account personalizzabile. L'utente non può modificare in alcun modo le impostazioni o le dimensioni dei widget, né aggiungere o rimuovere widget dal dashboard. È pertanto opportuno modificarli per l'utente, in modo che possa visualizzare le statistiche sulla protezione della rete. A tale scopo, nella scheda **Dashboard** è possibile eseguire con i widget le stesse azioni della sezione **Monitoraggio e generazione dei rapporti** → **Dashboard**:
   - Aggiungere nuovi widget al dashboard.
   - Nascondere i widget di cui l'utente non ha bisogno.
   - Spostare i widget in un ordine specifico.
   - Modificare le dimensioni o l'aspetto dei widget.
   - Modificare le impostazioni dei widget.
6. Spostare l'interruttore per abilitare l'opzione **Visualizza la console in modalità Solo dashboard**.

   Successivamente, sarà disponibile solo il dashboard per l'utente. Quest'ultimo può monitorare le statistiche ma non può modificare le impostazioni di protezione della rete e l'aspetto del dashboard. Poiché viene visualizzato lo stesso dashboard che appare all'utente, non è possibile modificarlo.

Se si mantiene l'opzione disabilitata, viene visualizzato il menu principale per l'utente, in modo che possa eseguire varie azioni in Kaspersky Security Center Linux, inclusa la modifica delle impostazioni di protezione e dei widget.

7. Fare clic sul pulsante **Salva** al termine della configurazione della modalità Solo dashboard. Solo successivamente l'utente visualizzerà il dashboard preconfigurato.

8. Se l'utente desidera visualizzare le statistiche delle applicazioni Kaspersky supportate e ha bisogno dei diritti di accesso per farlo, configurare i diritti per l'utente. Successivamente, l'utente può visualizzare i dati delle applicazioni Kaspersky nei widget di queste applicazioni.

Adesso l'utente può accedere a Kaspersky Security Center Linux con l'account personalizzato e monitorare le statistiche di protezione della rete in modalità Solo dashboard.

Rapporti

Questa sezione descrive come utilizzare i rapporti, gestire i modelli di rapporti personalizzati, utilizzare i modelli di rapporti per generarne di nuovi e creare attività di distribuzione dei rapporti.

Utilizzo dei rapporti

La funzionalità Rapporti consente di ottenere informazioni numeriche dettagliate sulla sicurezza della rete dell'organizzazione, nonché di salvare le informazioni in un file, inviarlo tramite e-mail e stamparlo.

I rapporti sono disponibili in Kaspersky Security Center Web Console, nella sezione **Monitoraggio e generazione dei rapporti**, facendo clic su **Rapporti**.

Per impostazione predefinita, i rapporti includono informazioni relative agli ultimi 30 giorni.

Kaspersky Security Center Linux dispone di un set predefinito di rapporti per le seguenti categorie:

- **Stato protezione**
- **Distribuzione**
- **Aggiornamento**
- **Statistiche delle minacce**
- **Altro**

È possibile creare modelli di rapporto personalizzati, modificare i modelli di rapporto ed eliminarli.

È possibile creare rapporti basati su modelli esistenti, esportare i rapporti in file e creare attività per l'invio dei rapporti.

Creazione di un modello di rapporto

Per creare un modello di rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuovo modello di rapporto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Immettere il nome del rapporto e selezionare il tipo di rapporto.
4. Nel passaggio **Ambito** della procedura guidata selezionare il set di dispositivi client (gruppo di amministrazione, selezione dispositivi, dispositivi selezionati o tutti i dispositivi nella rete) per cui visualizzare i dati nei rapporti basati su questo modello di rapporto.
5. Nel passaggio **Periodo di generazione del rapporto** della procedura guidata specificare il periodo del rapporto. I valori disponibili sono i seguenti:

   - Tra le due date specificate
   - Dalla data specificata alla data di creazione del rapporto
   - Dalla data di creazione del rapporto meno il numero specificato di giorni alla data di creazione del rapporto

   Questa pagina potrebbe non essere visualizzata per alcuni rapporti.
6. Fare clic su **OK** per chiudere la procedura guidata.
7. Eseguire una delle seguenti operazioni:

   - Fare clic sul pulsante **Salva ed esegui** per salvare il nuovo modello di rapporto ed eseguire un rapporto basato su di esso.

     Il modello di rapporto verrà salvato. Il rapporto verrà generato.
   - Fare clic sul pulsante **Salva** per salvare il nuovo modello di rapporto.

     Il modello di rapporto verrà salvato.

È possibile utilizzare il nuovo modello per la creazione e la visualizzazione dei rapporti.

Visualizzazione e modifica delle proprietà dei modelli di rapporto

È possibile visualizzare e modificare le proprietà di base di un modello di rapporto, ad esempio il nome del modello di rapporto o i campi visualizzati nel rapporto.

Per visualizzare e modificare le proprietà di un modello di rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Selezionare la casella di controllo accanto al modello di rapporto per cui si desidera visualizzare e modificare le proprietà.

   In alternativa, è possibile generare il rapporto e quindi fare clic sul pulsante **Modifica**.
3. Fare clic sul pulsante **Apri proprietà del modello di rapporto**.

   Verrà visualizzata la finestra **Modifica del rapporto <Nome rapporto>** con la scheda **Generale** selezionata.

4. Modificare le proprietà del modello di rapporto:

- Scheda **Generale**:
  - Nome del modello di rapporto
  - Numero massimo di voci da visualizzare

    Se questa opzione è abilitata, il numero di voci visualizzate nella tabella con i dati dettagliati del rapporto non supera il valore specificato. Si noti che questa opzione non influisce sul numero massimo di eventi che è possibile includere nel rapporto quando si esporta il rapporto in un file.

    Le voci nei rapporti vengono prima ordinate in base alle regole specificate nella sezione **Campi** → **Campi dettagli** delle proprietà del modello di rapporto, quindi vengono mantenute solo le prime voci risultanti. Il titolo della tabella con i dati dettagliati del rapporto mostra il numero di voci visualizzate e il numero totale di voci disponibili, corrispondenti alle altre impostazioni del modello di rapporto.

    Se questa opzione è disabilitata, la tabella con i dati dettagliati del rapporto conterrà tutte le voci disponibili. Non è consigliabile disabilitare questa opzione. La limitazione del numero di voci visualizzate nel rapporto consente di ridurre il carico sul sistema di gestione database (DBMS) e il tempo necessario per la creazione e l'esportazione del rapporto. Alcuni rapporti contengono un numero eccessivo di voci. In questi casi, potrebbe essere difficile leggerle e analizzarle tutte. Inoltre, nel dispositivo potrebbe verificarsi l'esaurimento della memoria durante la generazione di un rapporto e, in questo caso, non sarà possibile visualizzare il rapporto.

    Per impostazione predefinita, questa opzione è abilitata. Il valore predefinito è 1000.

  - **Gruppo**

    Fare clic sul pulsante **Impostazioni** per modificare il set di dispositivi client per cui viene creato il rapporto. Per alcuni tipi di rapporti, il pulsante potrebbe non essere disponibile. Le impostazioni effettive dipendono dalle impostazioni specificate durante la creazione del modello di rapporto.

  - **Intervallo**

    Fare clic sul pulsante **Impostazioni** per modificare il periodo del rapporto. Per alcuni tipi di rapporti, il pulsante potrebbe non essere disponibile. I valori disponibili sono i seguenti:

    - Tra le due date specificate
    - Dalla data specificata alla data di creazione del rapporto
    - Dalla data di creazione del rapporto meno il numero specificato di giorni alla data di creazione del rapporto

  - Includi i dati degli Administration Server secondari e virtuali

    Se questa opzione è abilitata, il rapporto include le informazioni ottenute dagli Administration Server secondari e virtuali subordinati all'Administration Server per cui viene creato il modello di rapporto.

    Disabilitare questa opzione per visualizzare solo i dati relativi all'Administration Server corrente.

    Per impostazione predefinita, questa opzione è abilitata.

  - Fino al livello di nidificazione

Il rapporto include i dati degli Administration Server secondari e virtuali posizionati al di sotto dell'Administration Server corrente a un livello di nidificazione minore o uguale al valore specificato.

Il valore predefinito è 1. È consigliabile modificare questo valore se è necessario recuperare informazioni da Administration Server secondari posizionati a livelli inferiori della struttura.

- Intervallo di attesa dati (min.)

  Prima della generazione del rapporto, l'Administration Server per cui viene creato il modello di rapporto attende i dati dagli Administration Server secondari per il numero di minuti specificato. Se non viene ricevuto alcun dato da un Administration Server secondario al termine di questo periodo, il rapporto viene eseguito comunque. Anziché i dati effettivi, il rapporto mostra i dati recuperati dalla cache (se è abilitata l'opzione **Salva nella cache i dati degli Administration Server secondari**) oppure **N/D** (non disponibile) in caso contrario.

  Il valore predefinito è 5 (minuti).

- Salva nella cache i dati degli Administration Server secondari

  Gli Administration Server secondari trasferiscono regolarmente i dati all'Administration Server per cui viene creato il modello di rapporto. I dati trasferiti vengono quindi archiviati nella cache.

  Se l'Administration Server corrente non riesce a ricevere i dati da un Administration Server secondario durante la generazione del rapporto, il rapporto mostra i dati recuperati dalla cache. Verrà anche visualizzata la data in cui i dati sono stati trasferiti nella cache.

  Se questa opzione è abilitata, è possibile visualizzare le informazioni dagli Administration Server secondari, anche se non è possibile recuperare i dati aggiornati. I dati visualizzati potrebbero tuttavia essere obsoleti.

  Per impostazione predefinita, questa opzione è disabilitata.

- Frequenza di aggiornamento cache (ore)

  A intervalli regolari gli Administration Server secondari trasferiscono i dati all'Administration Server per cui viene creato il modello di rapporto. È possibile specificare questo periodo in ore. Se si specificano 0 ore, i dati vengono trasferiti solo al momento della generazione del rapporto.

  Il valore predefinito è 0.

- Trasferisci informazioni dettagliate dagli Administration Server secondari

  Nel rapporto generato, la tabella con i dati dettagliati del rapporto include i dati ottenuti dagli Administration Server secondari dell'Administration Server per cui viene creato il modello di rapporto.

  L'abilitazione di questa opzione rallenta la generazione dei rapporti e aumenta il traffico tra gli Administration Server. È tuttavia possibile visualizzare tutti i dati in un solo rapporto.

  Anziché attivare questa opzione, può essere preferibile analizzare i dati dettagliati del rapporto per identificare un Administration Server secondario che presenta problemi e quindi generare lo stesso rapporto solo per tale Administration Server.

  Per impostazione predefinita, questa opzione è disabilitata.

- Scheda **Campi**

Selezionare i campi che verranno visualizzati nel rapporto e utilizzare i pulsanti **Sposta su** e **Sposta giù** per modificare l'ordine dei campi. Utilizzare il pulsante **Aggiungi** o **Modifica** per specificare se le informazioni nel rapporto devono essere ordinate e filtrate in base a ciascuno dei campi.

Nella sezione **Filtri di Campi dettagli** è inoltre possibile fare clic sul pulsante **Converti filtri** per iniziare a utilizzare il formato di filtro esteso. Questo formato consente di combinare le condizioni di filtro specificate in vari campi utilizzando l'operatore logico OR. Dopo aver fatto clic sul pulsante, il pannello **Converti filtri** si aprirà a destra. Fare clic sul pulsante **Converti filtri** per confermare la conversione. Adesso è possibile definire un filtro convertito con condizioni dalla sezione **Campi dettagli** che vengono applicate utilizzando l'operatore logico OR.

La conversione di un rapporto nel formato che supporta condizioni di filtro complesse renderà il rapporto incompatibile con le versioni precedenti di Kaspersky Security Center (11 e precedenti). Inoltre, il rapporto convertito non conterrà alcun dato degli Administration Server secondari che eseguono le versioni incompatibili.

5. Fare clic su **Salva** per salvare le modifiche.
6. Chiudere la finestra **Modifica del rapporto <nome rapporto>**.

Il modello di rapporto aggiornato verrà visualizzato nell'elenco dei modelli di rapporto.

Esportazione di un rapporto in un file

È possibile salvare uno o più rapporti in formato XML, HTML o PDF. Kaspersky Security Center Linux consente di esportare contemporaneamente fino a 10 rapporti in file del formato specificato.

Per esportare un rapporto in un file:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Rapporti**.
2. Scegliere i rapporti da esportare.

   Se si scelgono più di 10 rapporti, il pulsante **Esporta rapporto** verrà disabilitato.
3. Fare clic sul pulsante **Esporta rapporto**.
4. Nella finestra visualizzata specificare i seguenti parametri di esportazione:

   - **Nome file**.

     Se si seleziona un rapporto da esportare, specificare il nome del file del rapporto.

     Se si seleziona più di un rapporto, i nomi dei file dei rapporti coincideranno con il nome dei modelli di rapporto selezionati.

   - **Numero massimo di voci**.

     Specificare il numero massimo di voci incluse nel file del rapporto. Il valore predefinito è 10.000.

     È possibile esportare un rapporto con un numero illimitato di voci. Si noti che se il rapporto contiene un numero elevato di voci, il tempo necessario per generarlo ed esportarlo aumenta.

   - **Formato file**.

     Selezionare il formato del file del rapporto: XML, HTML o PDF. Se si esportano più rapporti, tutti i rapporti selezionati vengono salvati nel formato specificato come file separati.

Lo strumento wkhtmltopdf è necessario per convertire un rapporto in formato PDF. Quando si seleziona l'opzione PDF, Administration Server verifica se lo strumento wkhtmltopdf è installato nel dispositivo. Se lo strumento non è installato, l'applicazione mostra un messaggio in cui si richiede di installare lo strumento nel dispositivo Administration Server. Installare lo strumento manualmente, quindi continuare con il passaggio successivo.

5. Fare clic sul pulsante **Esporta rapporto**.

Il rapporto viene salvato in un file nel formato specificato.

Generazione e visualizzazione di un rapporto

Per creare e visualizzare un rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Fare clic sul nome del modello di rapporto che si desidera utilizzare per creare un rapporto.

   Verrà generato e visualizzato un rapporto che utilizza il modello selezionato.

I dati del rapporto vengono visualizzati in base alla localizzazione impostata per Administration Server.

Nei rapporti generati, alcuni tipi di carattere potrebbero essere visualizzati in modo errato sui diagrammi. Per risolvere questo problema, installare la libreria fontconfig. Inoltre, verificare che i tipi di carattere corrispondenti alle impostazioni locali del sistema operativo siano installati nel sistema operativo.

Il rapporto include i seguenti dati:

- Nella scheda **Riepilogo**:
  - Nome e tipo di rapporto, breve descrizione e periodo di generazione del rapporto, oltre che informazioni sul gruppo di dispositivi per cui è stato generato il rapporto.
  - Grafico con i dati più significativi del rapporto.
  - Tabella consolidata con indicatori del rapporto calcolati.
- Nella scheda **Dettagli** viene visualizzata una tabella con dati dettagliati sul rapporto.

Creazione di un'attività di invio dei rapporti

È possibile creare un'attività per l'invio dei rapporti selezionati.

Per creare un'attività di invio dei rapporti:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.

2. [Facoltativo] Selezionare le caselle di controllo accanto ai modelli di rapporto per cui si desidera creare un'attività di invio dei rapporti.

3. Fare clic sul pulsante **Nuova attività di invio rapporti**.

4. Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

5. Nella prima pagina della procedura guidata immettere il nome dell'attività. Il nome predefinito è **Invia rapporti (<N>)**, dove <N> è il numero progressivo dell'attività.

6. Nella pagina delle impostazioni dell'attività della procedura guidata specificare le seguenti impostazioni:

   a. Modelli di rapporti che devono essere inviati dall'attività. Se sono stati selezionati nel passaggio 2, ignorare questo passaggio.

   b. Formato del rapporto: HTML, XLS o PDF.

      Lo strumento wkhtmltopdf è necessario per convertire un rapporto in formato PDF. Quando si seleziona l'opzione PDF, Administration Server verifica se lo strumento wkhtmltopdf è installato nel dispositivo. Se lo strumento non è installato, l'applicazione mostra un messaggio in cui si richiede di installare lo strumento nel dispositivo Administration Server. Installare lo strumento manualmente, quindi continuare con il passaggio successivo.

   c. Se i rapporti devono essere inviati tramite e-mail, insieme alle impostazioni di notifica tramite e-mail.

   d. Se i rapporti devono essere salvati in una cartella, insieme alle impostazioni corrispondenti.

      Dopo aver abilitato l'opzione **Salva rapporti nella cartella**, è necessario specificare un percorso POSIX per la cartella. Se si desidera salvare i rapporti in una cartella condivisa, è necessario selezionare anche la casella di controllo **Specifica l'account per accedere alla cartella condivisa**, quindi specificare l'account utente e la password per accedere a questa cartella.

      > Se si sceglie di salvare i rapporti in una cartella condivisa, è necessario garantire l'accesso a questa cartella dal dispositivo su cui è installato Administration Server. Le modalità per garantire l'accesso e gli strumenti utilizzati dipendono dall'infrastruttura dell'utente.

      Quando si salvano i rapporti in una cartella locale, in genere non sono necessarie credenziali, poiché l'account con cui è in esecuzione Administration Server ha accesso a questa cartella. Se necessario, è possibile specificare le credenziali utente nel passaggio **Selezione di un account per l'esecuzione dell'attività** della procedura guidata.

      Indipendentemente dalla cartella scelta, è anche possibile selezionare la casella di controllo **Sovrascrivi i rapporti precedenti dello stesso tipo** se si desidera che il nuovo file dei rapporti sovrascriva il file salvato nella cartella dei rapporti all'avvio dell'attività precedente.

7. Se si desidera modificare altre impostazioni dell'attività dopo averla creata, nella pagina **Completa creazione attività** della procedura guidata abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione**.

8. Fare clic sul pulsante **Crea** per creare l'attività e chiudere la procedura guidata.

   Verrà creata l'attività di invio dei rapporti. Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata la finestra delle impostazioni dell'attività.

Eliminazione di modelli di rapporto

Per eliminare uno o più modelli di rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Rapporti**.
2. Selezionare le caselle di controllo accanto ai modelli di rapporto che si desidera eliminare.
3. Fare clic sul pulsante **Elimina**.
4. Nella finestra visualizzata fare clic su **OK** per confermare la selezione.

I modelli di rapporto selezionati verranno eliminati. Se questi modelli di rapporto sono stati inclusi nelle attività di invio dei rapporti, verranno rimossi anche dalle attività.

Eventi e selezioni di eventi

Questa sezione fornisce informazioni sugli eventi e sulle selezioni di eventi, sui tipi di eventi che si verificano nei componenti di Kaspersky Security Center Linux e sulla gestione del blocco degli eventi frequenti.

Informazioni sugli eventi in Kaspersky Security Center Linux

Kaspersky Security Center Linux consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Le informazioni sugli eventi vengono salvate nel database di Administration Server.

Eventi in base al tipo

In Kaspersky Security Center Linux sono disponibili i seguenti tipi di eventi:

- Eventi generici. Questi eventi si verificano in tutte le applicazioni Kaspersky gestite. Un esempio di evento generico è l'Epidemia di virus. Gli eventi generici hanno sintassi e semantica rigorosamente definite. Gli eventi generici vengono ad esempio utilizzati nei rapporti e nei dashboard.
- Eventi specifici delle applicazioni gestiti da Kaspersky. Ogni applicazione Kaspersky gestita dispone di uno specifico set di eventi.

Eventi in base alla sorgente

È possibile visualizzare l'elenco completo degli eventi che possono essere generati da un'applicazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare l'elenco degli eventi nelle proprietà dell'Administration Server.

Gli eventi possono essere generati dalle seguenti applicazioni:

- Componenti di Kaspersky Security Center Linux:
  - Administration Server
  - Network Agent

- Applicazioni Kaspersky gestite

  Per i dettagli sugli eventi generati dalle applicazioni gestite da Kaspersky, consultare la documentazione dell'applicazione corrispondente.

Eventi in base al livello di importanza

Ogni evento dispone di uno specifico livello di importanza. In base alle condizioni in cui si verifica, a un evento possono essere assegnati diversi livelli di importanza. Esistono quattro livelli di importanza degli eventi:

- Un *evento critico* è un evento che indica la presenza di un problema critico che può determinare una perdita dei dati, un malfunzionamento o un errore critico.
- Un *errore funzionale* è un evento che indica la presenza di un problema grave, un errore o un malfunzionamento che si è verificato durante l'esecuzione dell'applicazione o di una procedura.
- Un *avviso* è un evento che non è necessariamente grave, ma indica comunque un potenziale problema futuro. La maggior parte degli eventi viene designata come avviso se l'applicazione può essere ripristinata senza perdite di dati o funzionalità importanti dopo che si sono verificati tali eventi.
- Un *evento informativo* è un evento che si verifica allo scopo di segnalare il completamento di un'operazione, il corretto funzionamento dell'applicazione o il completamento di una procedura.

Ogni evento ha un periodo di archiviazione definito, durante il quale può essere visualizzato o modificato in Kaspersky Security Center Linux. Alcuni eventi non vengono salvati nel database di Administration Server per impostazione predefinita, poiché il relativo periodo di archiviazione definito è pari a zero. Solo gli eventi che verranno memorizzati nel database di Administration Server per almeno un giorno possono essere esportati in sistemi esterni.

Eventi dei componenti di Kaspersky Security Center Linux

Ogni componente Kaspersky Security Center Linux dispone di uno specifico set di tipi di eventi. Questa sezione elenca i tipi di eventi che si verificano nell'Administration Server e nel Network Agent di Kaspersky Security Center. I tipi di eventi che si verificano nelle applicazioni Kaspersky non sono elencati in questa sezione.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Struttura dei dati della descrizione del tipo di evento

Per ogni tipo di evento, sono indicati il relativo nome visualizzato, l'identificatore (ID), il codice alfabetico, la descrizione e il periodo di archiviazione predefinito.

- **Nome visualizzato del tipo di evento**. Questo testo è visualizzato in Kaspersky Security Center Linux durante la configurazione degli eventi e quando gli eventi si verificano.
- **ID del tipo di evento**. Questo codice numerico viene utilizzato durante l'elaborazione degli eventi tramite strumenti di terzi per l'analisi degli eventi.

- **Tipo di evento** (codice alfabetico). Questo codice viene utilizzato quando si esplorano e si elaborano gli eventi con le visualizzazione pubbliche disponibili nel database di Kaspersky Security Center Linux e quando gli eventi vengono esportati in un sistema SIEM.

- **Descrizione**. Questo testo contiene le situazioni in cui si verifica un evento e come procedere in questo caso.

- **Periodo di archiviazione predefinito**. Rappresenta il numero di giorni per cui l'evento viene memorizzato nel database di Administration Server ed è visualizzato nell'elenco degli eventi in Administration Server. Al termine di questo periodo, l'evento viene eliminato. Se il valore per il periodo di archiviazione degli eventi è 0, gli eventi vengono rilevati ma non sono visualizzati nell'elenco degli eventi in Administration Server. Se è stato configurato il salvataggio di tali eventi nel registro eventi del sistema operativo, è possibile accedervi in tale posizione.

  È possibile modificare il periodo di archiviazione per gli eventi: Impostazione del periodo di archiviazione per un evento

Eventi di Administration Server

Questa sezione contiene informazioni sugli eventi relativi ad Administration Server.

Eventi critici di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Administration Server con il livello di importanza **Critico**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi critici di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
È stato superato il limite di licenze	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Una volta al giorno Kaspersky Security Center Linux verifica se è stato superato un limite di licenze. Gli eventi di questo tipo si verificano quando Administration Server rileva il superamento di alcune limitazioni di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client e se il numero delle unità di licensing attualmente utilizzate coperte da una singola licenza supera il 110% del numero totale di unità coperte dalla licenza. Anche quando si verifica questo evento, i dispositivi client sono protetti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare i dispositivi non in uso. • Fornire una licenza per più dispositivi (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). Kaspersky Security Center Linux determina le regole per generare gli eventi quando viene superato un limite di licenze.	180 giorni
Il dispositivo è diventato	4111	KLSRV_HOST_OUT_CONTROL	Eventi di questo tipo si verificano se un dispositivo gestito è visibile nella rete ma non si connette ad Administration Server da un periodo specifico.	180 giorni

non gestito			Determinare il motivo che impedisce il corretto funzionamento di Network Agent nel dispositivo. Le cause possibili includono i problemi di rete e la rimozione di Network Agent dal dispositivo.	
Lo stato del dispositivo è Critico	4113	KLSRV_HOST_STATUS_CRITICAL	Eventi di questo tipo si verificano quando a un dispositivo gestito viene assegnato lo stato *Critico*. È possibile configurare le condizioni in cui lo stato del dispositivo diventa *Critico*.	180 giorni
Il file chiave è stato aggiunto alla lista vietati	4124	KLSRV_LICENSE_BLACKLISTED	Eventi di questo tipo si verificano quando Kaspersky ha aggiunto il codice di attivazione o il file chiave in uso alla lista vietati. Contattare il Servizio di assistenza tecnica per ulteriori dettagli.	180 giorni
La licenza sta per scadere	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Eventi di questo tipo si verificano quando si avvicina la data di scadenza della licenza commerciale. Una volta al giorno Kaspersky Security Center Linux verifica se si è in prossimità della data di scadenza della licenza. Gli eventi di questo tipo vengono pubblicati 30 giorni, 15 giorni, 5 giorni e 1 giorno prima della data di scadenza della licenza. Questo numero di giorni non può essere modificato. Se Administration Server è disattivato nel giorno specificato prima della data di scadenza della licenza, l'evento non verrà pubblicato fino al giorno successivo. Alla scadenza della licenza commerciale, Kaspersky Security Center Linux fornisce solo le funzionalità di base. È possibile rispondere all'evento nei seguenti modi: • Verificare di aver aggiunto una chiave di licenza di riserva ad Administration Server. • Se si utilizza un abbonamento, assicurarsi di rinnovarlo. L'abbonamento illimitato viene rinnovato automaticamente se il pagamento al provider di servizi è stato effettuato anticipatamente entro il termine.	180 giorni
Il certificato è scaduto	4132	KLSRV_CERTIFICATE_EXPIRED	Eventi di questo tipo si verificano allo scadere del certificato di Administration Server per Mobile Device Management. È necessario aggiornare il certificato scaduto.	180 giorni

Eventi di errore funzionale di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Administration Server con il livello di importanza **Errore funzionale**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di errore funzionale di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Errore di runtime	4125	KLSRV_RUNTIME_ERROR	Eventi di questo tipo si verificano a causa di problemi sconosciuti. La maggior parte delle volte si tratta di problemi DBMS, problemi di rete e altri problemi hardware e software. È possibile trovare i dettagli dell'evento nella descrizione dell'evento.	180 giorni

Impossibile copiare gli aggiornamenti nella cartella specificata	4123	KLSRV_UPD_REPL_FAIL	Eventi di questo tipo si verificano quando gli aggiornamenti software vengono copiati in una cartella condivisa aggiuntiva. È possibile rispondere all'evento nei seguenti modi: • Verificare che l'account utente utilizzato per ottenere l'accesso alla cartella disponga dell'autorizzazione di scrittura. • Verificare eventuali variazioni del nome utente e/o della password della cartella. • Verificare la connessione Internet poiché potrebbe essere la causa dell'evento. Seguire le istruzioni per l'aggiornamento dei database e dei moduli software.	180 giorni
Spazio su disco esaurito	4107	KLSRV_DISK_FULL	Eventi di questo tipo si verificano quando nel disco rigido del dispositivo in cui è installato Administration Server si esaurisce lo spazio disponibile. Liberare spazio su disco nel dispositivo.	180 giorni
La cartella condivisa non è disponibile	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Eventi di questo tipo si verificano se la cartella condivisa di Administration Server non è disponibile. È possibile rispondere all'evento nei seguenti modi: • Verificare che Administration Server (dove si trova la cartella condivisa) sia attivato e disponibile. • Verificare eventuali variazioni del nome utente e/o della password della cartella. • Verificare la connessione di rete.	180 giorni
Database di Administration Server non disponibile	4109	KLSRV_DATABASE_UNAVAILABLE	Eventi di questo tipo si verificano se il database di Administration Server diventa non disponibile. È possibile rispondere all'evento nei seguenti modi: • Verificare se è disponibile il server remoto in cui è installato DBMS. • Visualizzare i log DBMS per scoprire il motivo della mancata disponibilità di Administration Server.	180 giorni
Spazio disponibile esaurito nel database di Administration Server	4110	KLSRV_DATABASE_FULL	Eventi di questo tipo si verificano quando non è disponibile spazio nel database di Administration Server. Administration Server non funziona quando il database ha raggiunto la capacità massima e non è possibile eseguire ulteriori registrazioni nel database. Di seguito sono riportate le cause di questo evento, a seconda del DBMS in uso, e le risposte appropriate all'evento: • Limitare il numero di eventi da archiviare nel database di Administration Server. • Nel database di Administration Server sono presenti troppi eventi inviati dal componente Controllo Applicazioni. È possibile modificare le impostazioni del criterio di Kaspersky Endpoint Security relative all'archiviazione degli eventi di	180 giorni

			Controllo Applicazioni nel database di Administration Server. Rivedere le informazioni sulla selezione DBMS.	
Impossibile eseguire il polling del segmento cloud	4143	KLSRV_KLCLOUD_SCAN_ERROR	Eventi di questo tipo si verificano quando l'Administration Server non riesce a eseguire il polling di un segmento di rete in un ambiente cloud. Leggere i dettagli nella descrizione dell'evento e rispondere di conseguenza.	Non archiviato

Eventi di avviso di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Administration Server con il livello di importanza **Avviso**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di avviso di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
È stato rilevato un evento frequente		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Eventi di questo tipo si verificano quando Administration Server rileva un evento frequente in un dispositivo gestito. Per ulteriori dettagli, consultare la sezione seguente: Blocco degli eventi frequenti.	90 giorni
È stato superato il limite di licenze	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una volta al giorno Kaspersky Security Center Linux verifica se è stato superato un limite di licenze. Gli eventi di questo tipo si verificano quando Administration Server rileva il superamento di alcune limitazioni di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client e se il numero delle unità di licensing attualmente utilizzate coperte da una singola licenza costituisce dal 100% al 110% del numero totale di unità coperte dalla licenza. Anche quando si verifica questo evento, i dispositivi client sono protetti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare i dispositivi non in uso. • Fornire una licenza per più dispositivi (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). Kaspersky Security Center Linux determina le regole per generare gli eventi quando viene superato un limite di licenze.	90 giorni
Il dispositivo è rimasto inattivo nella rete per molto tempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Eventi di questo tipo si verificano quando un dispositivo gestito risulta inattivo per un determinato periodo di tempo. Molto spesso ciò accade quando un dispositivo gestito viene disattivato. È possibile rispondere all'evento nei seguenti modi: • Rimuovere manualmente il dispositivo dall'elenco dei dispositivi gestiti.	90 giorni

			Specificare l'intervallo di tempo dopo il quale viene creato l'evento **Il dispositivo è rimasto inattivo nella rete per molto tempo** utilizzando Kaspersky Security Center Web Console. • Specificare l'intervallo di tempo dopo il quale il dispositivo viene automaticamente rimosso dal gruppo utilizzando Kaspersky Security Center Web Console.	
Conflitto dei nomi di dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Eventi di questo tipo si verificano quando Administration Server considera due o più dispositivi gestiti come un unico dispositivo. Molto spesso questo accade quando un disco rigido clonato è stato utilizzato per la distribuzione del software nei dispositivi gestiti e senza eseguire il passaggio di Network Agent alla modalità di clonazione del disco dedicata in un dispositivo di riferimento. Per evitare questo problema, eseguire il passaggio di Network Agent alla modalità di clonazione del disco in un dispositivo di riferimento prima di clonare il disco rigido di questo dispositivo.	90 giorni
Lo stato del dispositivo è Avviso	4114	KLSRV_HOST_STATUS_WARNING	Eventi di questo tipo si verificano quando a un dispositivo gestito viene assegnato lo stato *Avviso*. È possibile configurare le condizioni in cui lo stato del dispositivo diventa *Avviso*.	90 giorni
Il certificato è stato richiesto	4133	KLSRV_CERTIFICATE_REQUESTED	Eventi di questo tipo si verificano quando un certificato per Mobile Device Management non viene riemesso automaticamente. Di seguito sono elencate le possibili cause e le risposte appropriate all'evento: • È stata avviata la riemissione automatica per un certificato per il quale l'opzione **Riemetti automaticamente il certificato se possibile** è disabilitata. Ciò potrebbe essere dovuto a un errore che si è verificato durante la creazione del certificato. Potrebbe essere necessaria la riemissione manuale del certificato. • Se si utilizza un'integrazione con un'infrastruttura a chiave pubblica, la causa potrebbe essere un attributo SAM-Account-Name mancante dell'account utilizzato per l'integrazione con PKI e per l'emissione del certificato. Esaminare le proprietà dell'account.	90 giorni
Il certificato è stato rimosso	4134	KLSRV_CERTIFICATE_REMOVED	Eventi di questo tipo si verificano quando un amministratore rimuove qualsiasi tipo di certificato (generale, posta, VPN) per Mobile Device Management. Dopo aver rimosso un certificato, i dispositivi mobili connessi tramite questo certificato non riusciranno a connettersi ad Administration Server. Questo evento potrebbe essere utile quando si esaminano malfunzionamenti associati alla gestione dei dispositivi mobili.	90 giorni

Il certificato APNs è scaduto	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Eventi di questo tipo si verificano allo scadere di un certificato APNs. È necessario rinnovare manualmente il certificato APNs e installarlo in un Server per dispositivi mobili MDM iOS.	Non archiviato
Il certificato APNs sta per scadere	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Eventi di questo tipo si verificano quando mancano meno di 14 giorni allo scadere del certificato APNs. Allo scadere del certificato APNs, è necessario rinnovare manualmente il certificato APNs e installarlo in un Server per dispositivi mobili MDM iOS. È consigliabile pianificare il rinnovo del certificato APNs prima della data di scadenza.	Non archiviato
Impossibile inviare il messaggio FCM al dispositivo mobile	4138	KLSRV_GCM_DEVICE_ERROR	Eventi di questo tipo si verificano quando Mobile Device Management è configurato per l'utilizzo di Google Firebase Cloud Messaging (FCM) per la connessione a dispositivi mobili gestiti con un sistema operativo Android e FCM Server non riesce a gestire alcune delle richieste ricevute da Administration Server. Questo vuol dire che alcuni dei dispositivi mobili gestiti non riceveranno una notifica push. Leggere il codice HTTP nei dettagli della descrizione dell'evento e rispondere di conseguenza. Per ulteriori informazioni sui codici HTTP ricevuti da FCM Server e sugli errori correlati, fare riferimento alla documentazione del servizio Google Firebase (vedere il capitolo "Codici di risposta dell'errore dei messaggi downstream").	90 giorni
Errore HTTP durante l'invio del messaggio FCM al server FCM	4139	KLSRV_GCM_HTTP_ERROR	Eventi di questo tipo si verificano quando Mobile Device Management è configurato per l'utilizzo di Google Firebase Cloud Messaging (FCM) per la connessione dei dispositivi mobili gestiti con il sistema operativo Android e FCM Server ripristina in Administration Server una richiesta con un codice HTTP diverso da 200 (OK). Di seguito sono elencate le possibili cause e le risposte appropriate all'evento: • Problemi sul lato server FCM. Leggere il codice HTTP nei dettagli della descrizione dell'evento e rispondere di conseguenza. Per ulteriori informazioni sui codici HTTP ricevuti da FCM Server e sugli errori correlati, fare riferimento alla documentazione del servizio Google Firebase (vedere il capitolo "Codici di risposta dell'errore dei messaggi downstream"). • Problemi sul lato server proxy (se si utilizza un server proxy). Leggere il codice HTTP nei dettagli dell'evento e rispondere di conseguenza.	90 giorni
Impossibile inviare il messaggio FCM al server FCM	4140	KLSRV_GCM_GENERAL_ERROR	Eventi di questo tipo si verificano a causa di errori imprevisti sul lato Administration Server quando si utilizza il protocollo HTTP di Google Firebase Cloud Messaging. Leggere i dettagli nella descrizione dell'evento e rispondere di conseguenza. Se non si riesce a trovare autonomamente la soluzione a un problema, è consigliabile contattare il Servizio di assistenza tecnica Kaspersky.	90 giorni
Poco spazio libero nel disco rigido	4105	KLSRV_NO_SPACE_ON_VOLUMES	Eventi di questo tipo si verificano quando nel disco rigido del dispositivo in cui è installato	90 giorni

			Administration Server si esaurisce quasi totalmente lo spazio disponibile. Liberare spazio su disco nel dispositivo.	
Spazio libero insufficiente nel database di Administration Server	4106	KLSRV_NO_SPACE_IN_DATABASE	Eventi di questo tipo si verificano se lo spazio in Administration Server è troppo limitato. Se non si ovvierà alla situazione, il database di Administration Server raggiungerà in breve tempo la capacità massima e Administration Server non funzionerà. Di seguito sono riportate le cause di questo evento, a seconda del DBMS in uso, e le risposte appropriate all'evento. Si utilizza il DBMS SQL Server Express Edition: • Nella documentazione di SQL Server Express esaminare il limite relativo alle dimensioni del database per la versione utilizzata. È probabile che il database di Administration Server stia per raggiungere il limite relativo alle dimensioni del database. • Limitare il numero di eventi da archiviare nel database di Administration Server. • Nel database di Administration Server sono presenti troppi eventi inviati dal componente Controllo Applicazioni. È possibile modificare le impostazioni del criterio di Kaspersky Endpoint Security relative all'archiviazione degli eventi di Controllo Applicazioni nel database di Administration Server. Si utilizza un DBMS diverso da SQL Server Express Edition: • Non limitare il numero di eventi da archiviare nel database di Administration Server • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server Rivedere le informazioni sulla selezione DBMS.	90 giorni
La connessione all'Administration Server secondario è stata interrotta	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Eventi di questo tipo si verificano quando una connessione all'Administration Server secondario viene interrotta. Leggere il registro del sistema operativo nel dispositivo in cui è installato l'Administration Server secondario e rispondere di conseguenza.	90 giorni
La connessione all'Administration Server primario è stata interrotta	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Eventi di questo tipo si verificano quando una connessione all'Administration Server primario viene interrotta. Leggere il registro del sistema operativo nel dispositivo in cui è installato l'Administration Server primario e rispondere di conseguenza.	90 giorni
Sono stati registrati nuovi aggiornamenti per i moduli software Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Eventi di questo tipo si verificano quando Administration Server registra nuovi aggiornamenti per il software Kaspersky installato nei dispositivi gestiti la cui installazione richiede l'approvazione. Approvare o rifiutare gli aggiornamenti utilizzando Kaspersky Security Center Web Console.	90 giorni
Poiché è stato superato il limite relativo al numero di eventi nel database, è stata avviata l'eliminazione degli eventi	4145	KLSRV_EVP_DB_TRUNCATING	Eventi di questo tipo si verificano quando viene avviata l'eliminazione degli eventi precedenti dal database di Administration Server dopo il raggiungimento della capacità massima del database di Administration Server. È possibile rispondere all'evento nei seguenti modi:	Non archiviato

			• Cambiare il numero massimo di eventi archiviati nel database di Administration Server • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server	
Poiché è stato superato il limite relativo al numero di eventi nel database, gli eventi sono stati eliminati	4146	KLSRV_EVP_DB_TRUNCATED	Eventi di questo tipo si verificano dopo l'eliminazione degli eventi precedenti dal database di Administration Server in seguito al raggiungimento della capacità massima del database di Administration Server. È possibile rispondere all'evento nei seguenti modi: • Cambiare il numero massimo consentito di eventi archiviati nel database di Administration Server • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server	Non archiviato

Eventi informativi di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Administration Server con il livello di importanza **Informazioni**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi informativi di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito	Osservazioni
Utilizzo della chiave di licenza superiore al 90%	4097	KLSRV_EV_LICENSE_CHECK_90	30 giorni	Gli eventi di questo tipo si verificano quando Administration Server rileva che alcuni limiti di licenze stanno per essere superati dalle applicazioni Kaspersky installate nei dispositivi client e se il numero delle unità di licensing attualmente utilizzate coperte da una singola licenza rappresenta oltre il 90% del numero totale di unità coperte dalla licenza. Anche quando viene superato un limite di licenze, i dispositivi client sono protetti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare i dispositivi non in uso. • Fornire una licenza per più dispositivi (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). Kaspersky Security Center Linux determina le regole per generare gli eventi quando viene superato un limite di licenze.
Nuovo dispositivo rilevato	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 giorni	Eventi di questo tipo si verificano quando vengono rilevati nuovi dispositivi in rete.
Il dispositivo è stato aggiunto automaticamente al gruppo	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 giorni	Eventi di questo tipo si verificano quando i dispositivi sono stati assegnati a un gruppo in base alle regole di spostamento dei dispositivi.
Il dispositivo è stato rimosso dal gruppo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 giorni	

poiché inattivo nella rete per molto tempo				
Sono disponibili alcuni file da inviare a Kaspersky per l'analisi	4131	KLSRV_APS_FILE_APPEARED	30 giorni	
L'ID istanza FCM è stato modificato in questo dispositivo mobile	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 giorni	
Aggiornamenti copiati nella cartella specificata	4122	KLSRV_UPD_REPL_OK	30 giorni	
La connessione all'Administration Server secondario è stata stabilita	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 giorni	
La connessione all'Administration Server primario è stata stabilita	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 giorni	
I database sono stati aggiornati	4144	KLSRV_UPD_BASES_UPDATED	30 giorni	
Controllo: la connessione ad Administration Server è stata stabilita	4147	KLAUD_EV_SERVERCONNECT	30 giorni	Eventi di questo tipo si verificano quando un utente si connette ad Administration Server tramite Kaspersky Security Center Web Console. Questi eventi includono l'indirizzo IP del dispositivo in cui è installato Kaspersky Security Center Web Console Server.
Controllo: l'oggetto è stato modificato	4148	KLAUD_EV_OBJECTMODIFY	30 giorni	Questo evento monitora le modifiche nei seguenti oggetti: • Gruppo di amministrazione • Gruppo di protezione • Utente • Pacchetto • Attività • Criterio • Server • Server virtuale
Controllo: lo stato dell'oggetto è stato modificato	4150	KLAUD_EV_TASK_STATE_CHANGED	30 giorni	Ad esempio, questo evento si verifica quando un'attività non è riuscita con un errore.
Controllo: le impostazioni del gruppo sono state modificate	4149	KLAUD_EV_ADMGROUP_CHANGED	30 giorni	
Controllo: la connessione ad Administration Server è stata terminata	4151	KLAUD_EV_SERVERDISCONNECT	30 giorni	
Controllo: le proprietà dell'oggetto sono state modificate	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 giorni	Questo evento monitora le modifiche nelle seguenti proprietà: • Utente

				• Licenza • Server • Server virtuale
Controllo: le autorizzazioni dell'utente sono state modificate	4153	KLAUD_EV_OBJECTACLMODIFIED	30 giorni	
Controllo: le chiavi di criptaggio sono state importate o esportate da Administration Server	5100	KLAUD_EV_DPEKEYSEXPORT	30 giorni	

Eventi di Network Agent

Questa sezione contiene informazioni sugli eventi relativi a Network Agent.

Eventi di avviso di Network Agent

La tabella seguente elenca gli eventi di Network Agent con il livello di gravità **Avviso**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di avviso di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Si è verificato un problema di sicurezza	549	GNRL_EV_APP_INCIDENT_OCCURED	Eventi di questo tipo si verificano quando viene rilevato un incidente in un dispositivo. Ad esempio, questo evento si verifica quando il dispositivo ha poco spazio su disco.	30 giorni
Proxy KSN avviato. Impossibile verificare la disponibilità di KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	Gli eventi di questo tipo si verificano quando la connessione di prova non riesce per la connessione proxy KSN configurata.	30 giorni
Installazione dell'aggiornamento software di terze parti rimandata	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	Ad esempio, eventi di questo tipo si verificano quando il Contratto di licenza con l'utente finale per un'installazione di aggiornamento di terze parti viene rifiutato.	30 giorni
Installazione dell'aggiornamento software di terze parti completata con un avviso	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	Scaricare i file di traccia e controllare il valore del campo KLRI_PATCH_RES_DESC per i dettagli.	30 giorni
È stato restituito un avviso durante l'installazione dell'aggiornamento dei moduli software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	Scaricare i file di traccia e controllare il valore del campo KLRI_PATCH_RES_DESC per i dettagli.	30 giorni

Eventi informativi di Network Agent

La tabella seguente elenca gli eventi di Network Agent con il livello di criticità **Informazioni**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi informativi di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Applicazione installata	7703	KLNAG_EV_INV_APP_INSTALLED	30 giorni
Applicazione rimossa	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 giorni
Applicazione monitorata installata	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 giorni
Applicazione monitorata rimossa	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 giorni
Nuovo dispositivo aggiunto	7708	KLNAG_EV_DEVICE_ARRIVAL	30 giorni
Dispositivo rimosso	7709	KLNAG_EV_DEVICE_REMOVE	30 giorni
Nuovo dispositivo rilevato	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 giorni
Dispositivo autorizzato	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 giorni
Proxy KSN avviato. La verifica della disponibilità di KSN è stata completata	7719	KSNPROXY_STARTED_CON_CHK_OK	30 giorni
Proxy KSN arrestato	7720	KSNPROXY_STOPPED	30 giorni
Applicazione di terze parti installata	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 giorni
Installazione dell'aggiornamento software di terze parti completata	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 giorni
Installazione dell'aggiornamento software di terze parti avviata	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 giorni
Installazione dell'aggiornamento dei moduli software avviata	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 giorni
Condivisione desktop Windows: applicazione avviata	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 giorni
Condivisione desktop Windows: file modificato	7713	KLUSRLOG_EV_FILE_MODIFIED	30 giorni
Condivisione desktop Windows: file letto	7712	KLUSRLOG_EV_FILE_READ	30 giorni
Condivisione desktop Windows: avviata	7715	KLUSRLOG_EV_WDS_BEGIN	30 giorni
Condivisione desktop Windows: arrestata	7716	KLUSRLOG_EV_WDS_END	30 giorni

Utilizzo di selezioni eventi

Le selezioni eventi consentono di visualizzare i set denominati degli eventi selezionati dal database di Administration Server. Questi set di eventi sono raggruppati in base alle seguenti categorie:

- In base al livello di importanza: **Eventi critici**, **Errori funzionali**, **Avvisi** e **Eventi informativi**
- In base al tempo: **Eventi recenti**
- In base al tipo: **Richieste utente** e **Eventi di controllo**

È possibile creare e visualizzare le selezioni eventi definite dall'utente in base alle impostazioni disponibili per la configurazione nell'interfaccia di Kaspersky Security Center Web Console.

Le selezioni eventi sono disponibili in Kaspersky Security Center Web Console, nella sezione **Monitoraggio e generazione dei rapporti**, facendo clic su **Selezioni eventi**.

Per impostazione predefinita, le selezioni eventi includono informazioni relative agli ultimi sette giorni.

Kaspersky Security Center Linux dispone di un set predefinito di selezioni eventi (preimpostate):

- Eventi con diversi livelli di importanza:
  - **Eventi critici**
  - **Errori funzionali**
  - **Avvisi**
  - **Eventi informativi**
- **Richieste utente** (eventi delle applicazioni gestite)
- **Eventi recenti** (nell'ultima settimana)
- **Eventi di controllo**.

È inoltre possibile creare e configurare ulteriori selezioni definite dall'utente. Nelle selezioni definite dall'utente è possibile filtrare gli eventi in base alle proprietà dei dispositivi da cui hanno avuto origine (nomi dei dispositivi, intervalli IP e gruppi di amministrazione), per tipi di eventi e livelli di criticità, per nome dell'applicazione e del componente e per intervallo di tempo. È anche possibile includere i risultati delle attività nell'ambito della ricerca. È inoltre disponibile un semplice campo di ricerca, in cui è possibile digitare una o più parole. Vengono visualizzati tutti gli eventi che contengono una delle parole digitate in qualsiasi punto dei relativi attributi (come nome dell'evento, descrizione o nome del componente).

Sia per le selezioni predefinite che per quelle definite dall'utente, è possibile limitare il numero di eventi visualizzati o il numero di record da cercare. Entrambe le opzioni influiscono sul tempo richiesto da Kaspersky Security Center Linux per visualizzare gli eventi. Più grande è il database, più tempo può richiedere il processo.

È possibile procedere come segue:

- Modificare le proprietà delle selezioni eventi
- Generare selezioni eventi
- Visualizzare i dettagli delle selezioni eventi
- Eliminare le selezioni eventi
- Eliminare gli eventi dal database di Administration Server

Creazione di una selezione eventi

Per creare una selezione eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Selezioni eventi**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Nuova selezione eventi** visualizzata specificare le impostazioni della nuova selezione eventi. Eseguire tale operazione in una o più sezioni della finestra.
4. Fare clic su **Salva** per salvare le modifiche.

   Verrà visualizzata la finestra di conferma.
5. Per visualizzare i risultati della selezione eventi, mantenere selezionata la casella di controllo **Vai al risultato della selezione**.
6. Fare clic su **Salva** per confermare la creazione della selezione eventi.

Se è stata mantenuta selezionata la casella di controllo **Vai al risultato della selezione**, verranno visualizzati i risultati della selezione eventi. In caso contrario, la nuova selezione eventi verrà visualizzata nell'elenco delle selezioni eventi.

Modifica di una selezione eventi

Per modificare una selezione eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Selezioni eventi**.
2. Selezionare la casella di controllo accanto alla selezione eventi che si desidera modificare.
3. Fare clic sul pulsante **Proprietà**.

   Verrà visualizzata una finestra delle impostazioni della selezione eventi.
4. Modificare le proprietà della selezione eventi.

   > Per le selezioni di eventi predefinite, è possibile modificare solo le proprietà nelle seguenti schede: **Generale** (tranne il nome della selezione), **Data/ora** e **Diritti di accesso**.

   Per le selezioni definite dall'utente, è possibile modificare tutte le proprietà.
5. Fare clic su **Salva** per salvare le modifiche.

La selezione eventi modificata verrà visualizzata nell'elenco.

Visualizzazione di un elenco di una selezione eventi

Per visualizzare una selezione eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Selezioni eventi**.
2. Selezionare la casella di controllo accanto alla selezione eventi che si desidera avviare.

3. Eseguire una delle seguenti operazioni:

   - Se si desidera configurare l'ordinamento dei risultati della selezione eventi, effettuare le seguenti operazioni:

     a. Fare clic sul pulsante **Riconfigura ordinamento e avvia**.

     b. Nella finestra **Riconfigurare l'ordinamento per la selezione eventi** visualizzata specificare le impostazioni di ordinamento.

     c. Fare clic sul nome della selezione.

   - In caso contrario, se si desidera visualizzare l'elenco degli eventi in base all'ordinamento in Administration Server, fare clic sul nome della selezione.

Verranno visualizzati i risultati della selezione eventi.

Esportazione di una selezione di eventi

Kaspersky Security Center Linux consente di salvare una selezione di eventi e le relative impostazioni in un file KLO. È possibile utilizzare questo file KLO per importare la selezione di eventi salvata sia per Kaspersky Security Center Windows che per Kaspersky Security Center Linux.

Si noti che è possibile esportare solo le selezioni di eventi definite dall'utente. Le selezioni di eventi dal set predefinito di Kaspersky Security Center Linux (selezioni predefinite) non possono essere salvate in un file.

Per esportare una selezione di eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.
2. Selezionare la casella di controllo accanto alla selezione eventi che si desidera esportare.

   Non è possibile esportare più selezioni di eventi contemporaneamente. Se si selezionano più selezioni, il pulsante **Esporta** verrà disabilitato.
3. Fare clic sul pulsante **Esporta**.
4. Nella finestra **Salva con nome** aperta, specificare il nome e il percorso del file della selezione di eventi, quindi fare clic sul pulsante **Salva**.

   La finestra **Salva con nome** viene visualizzata solo se si utilizza Google Chrome, Microsoft Edge oppure Opera. Se si utilizza un altro browser, il file della selezione di eventi viene salvato automaticamente nella cartella **Download**.

Importazione di una selezione di eventi

Kaspersky Security Center Linux consente di importare una selezione di eventi da un file KLO. Il file KLO contiene la selezione di eventi esportata e le sue impostazioni.

Per importare una selezione di eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.

2. Fare clic sul pulsante **Importa**, quindi scegliere una selezione di eventi che si desidera importare.

3. Nella finestra visualizzata, specificare il percorso del file KLO, quindi fare clic sul pulsante **Apri**. Si noti che è possibile selezionare solo una selezione di eventi.

   Viene avviata l'elaborazione della selezione di eventi.

Viene visualizzata la notifica con i risultati dell'importazione. Se la selezione di eventi viene importata correttamente, è possibile fare clic sul collegamento **Visualizza dettagli importazione** per visualizzare le proprietà della selezione di eventi.

Dopo un'importazione riuscita, la selezione di eventi viene visualizzata nell'elenco delle selezioni. Vengono importate anche le impostazioni della selezione di eventi.

Se la selezione di eventi appena importata ha un nome identico a quello di una selezione di eventi esistente, il nome della selezione importata viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Visualizzazione dei dettagli di un evento

Per visualizzare i dettagli di un evento:

1. Avviare una selezione eventi.

2. Fare clic sull'ora dell'evento desiderato.

   Verrà visualizzata la finestra **Proprietà evento**.

3. Nella finestra visualizzata è possibile eseguire le seguenti operazioni:

   - Visualizzare le informazioni sull'evento selezionato
   - Passare all'evento successivo e all'evento precedente nei risultati della selezione eventi
   - Passare al dispositivo in cui si è verificato l'evento
   - Passare al gruppo di amministrazione che include il dispositivo in cui si è verificato l'evento
   - Per un evento correlato a un'attività, passare alle proprietà dell'attività

Esportazione degli eventi in un file

Kaspersky Security Center Linux consente di salvare gli eventi da una selezione di eventi in un file TXT.

Per esportare gli eventi in un file:

1. Avviare una selezione eventi.

2. Selezionare la casella di controllo accanto all'evento desiderato.

È inoltre possibile selezionare più eventi o l'intera selezione di eventi.

3. Fare clic sul pulsante **Esporta in un file**.

L'evento selezionato verrà esportato in un file TXT.

Visualizzazione della cronologia di un oggetto da un evento

Da un evento di creazione o di modifica di un oggetto che supporta la gestione delle revisioni, è possibile passare alla cronologia delle revisioni dell'oggetto.

Per visualizzare la cronologia di un oggetto da un evento:

1. Avviare una selezione eventi.
2. Selezionare la casella di controllo accanto all'evento desiderato.
3. Fare clic sul pulsante **Cronologia revisioni**.

Verrà aperta la cronologia delle revisioni dell'oggetto.

Eliminazione di eventi

Per eliminare uno o più eventi:

1. Avviare una selezione eventi.
2. Selezionare le caselle di controllo accanto agli eventi desiderati.
3. Fare clic sul pulsante **Elimina**.

Gli eventi selezionati verranno eliminati e non potranno essere ripristinati.

Eliminazione di selezioni eventi

È possibile eliminare solo le selezioni eventi definite dall'utente. Le selezioni eventi predefinite non possono essere eliminate.

Per eliminare una o più selezioni eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Selezioni eventi**.
2. Selezionare le caselle di controllo accanto alle selezioni eventi che si desidera eliminare.
3. Fare clic su **Elimina**.

4. Nella finestra visualizzata fare clic su **OK**.

La selezione eventi verrà eliminata.

Impostazione del periodo di archiviazione per un evento

Kaspersky Security Center Linux consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Le informazioni sugli eventi vengono salvate nel database di Administration Server. Potrebbe essere necessario archiviare alcuni eventi per un periodo più o meno lungo di quanto specificato dai valori predefiniti. È possibile modificare le impostazioni predefinite del periodo di archiviazione per un evento.

Se non si è interessati all'archiviazione di alcuni eventi nel database di Administration Server, è possibile disabilitare l'impostazione appropriata nel criterio di Administration Server e nel criterio dell'applicazione Kaspersky o nelle proprietà di Administration Server (solo per gli eventi di Administration Server). Ciò consentirà di ridurre il numero dei tipi di eventi nel database.

Più lungo è il periodo di archiviazione per un evento, più velocemente il database raggiunge la capacità massima. Tuttavia, un periodo di archiviazione più lungo per un evento consente di eseguire le attività di monitoraggio e generazione dei rapporti per un periodo superiore.

Per impostare il periodo di archiviazione per un evento nel database di Administration Server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul nome del criterio desiderato.

   È possibile selezionare un criterio per un'applicazione Kaspersky gestita, Network Agent o Administration Server. Per Administration Server, è inoltre possibile configurare il periodo di archiviazione degli eventi facendo clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server desiderato.
3. Selezionare la scheda **Configurazione eventi**.

   Verrà visualizzato un elenco dei tipi di eventi correlati alla sezione **Critico**. Se necessario, è possibile passare alla sezione **Errore funzionale**, **Avviso** o **Informazioni**.
4. Nell'elenco dei tipi di eventi nel riquadro destro fare clic sul collegamento per l'evento di cui si desidera modificare il periodo di archiviazione.

   Nella sezione **Registrazione eventi** della finestra visualizzata l'interruttore **Archivia nel database di Administration Server per (giorni)** è abilitata.
5. Nella casella di modifica sotto questo interruttore inserire il numero di giorni per l'archiviazione dell'evento.
6. Se non si desidera archiviare un evento nel database di Administration Server, disabilitare l'opzione **Archivia nel database di Administration Server per (giorni)**.

   Se si configurano gli eventi di Administration Server nella finestra delle proprietà di Administration Server e se le impostazioni degli eventi sono bloccate nel criterio di Kaspersky Security Center Administration Server, non è possibile ridefinire il valore del periodo di archiviazione per un evento.
7. Fare clic su **OK**, quindi, dopo aver chiuso il riquadro destro, fare clic sul pulsante **Salva**.

   La finestra delle proprietà del criterio verrà chiusa.

Da questo momento, quando Administration Server riceve e archivia gli eventi del tipo selezionato, questi avranno il periodo di archiviazione modificato. Administration Server non modifica il periodo di archiviazione degli eventi ricevuti in precedenza.

Blocco degli eventi frequenti

Questa sezione fornisce informazioni sulla gestione del blocco degli eventi frequenti e sulla rimozione del blocco degli eventi frequenti.

Informazioni sul blocco degli eventi frequenti

Un'applicazione gestita, ad esempio Kaspersky Endpoint Security for Linux, installata in uno o più dispositivi gestiti può inviare molti eventi dello stesso tipo ad Administration Server. La ricezione di eventi frequenti può sovraccaricare il database di Administration Server e sovrascrivere altri eventi. Administration Server inizia a bloccare gli eventi più frequenti quando il numero di tutti gli eventi ricevuti supera il limite specificato per il database.

Administration Server blocca la ricezione automatica degli eventi frequenti. Non è possibile bloccare autonomamente gli eventi frequenti o scegliere quali eventi bloccare.

Se si desidera scoprire se un evento è bloccato, è possibile visualizzare l'elenco delle notifiche o controllare se questo evento è presente nella sezione **Blocco degli eventi frequenti** delle proprietà di Administration Server. Se l'evento è bloccato, è possibile eseguire le seguenti operazioni:

- Se si desidera impedire la sovrascrittura del database, è possibile continuare a bloccare la ricezione di questo tipo di eventi.
- Se ad esempio si desidera individuare il motivo dell'invio degli eventi frequenti ad Administration Server, è possibile sbloccare gli eventi frequenti e continuare a ricevere comunque gli eventi di questo tipo.
- Se si desidera continuare a ricevere gli eventi frequenti finché non vengono nuovamente bloccati, è possibile rimuovere dal blocco gli eventi frequenti.

Gestione del blocco degli eventi frequenti

Administration Server blocca la ricezione automatica degli eventi frequenti, ma è possibile sbloccare e continuare a ricevere gli eventi frequenti. È inoltre possibile bloccare la ricezione degli eventi frequenti sbloccati in precedenza.

Per gestire il blocco degli eventi frequenti:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Blocco degli eventi frequenti**.

3. Nella sezione **Blocco degli eventi frequenti**:

- Se si desidera sbloccare la ricezione degli eventi frequenti:

  a. Selezionare gli eventi frequenti che si desidera sbloccare e fare clic sul pulsante **Escludi**.

  b. Fare clic sul pulsante **Salva**.

- Se si desidera bloccare la ricezione degli eventi frequenti:

  a. Selezionare gli eventi frequenti che si desidera bloccare e fare clic sul pulsante **Blocca**.

  b. Fare clic sul pulsante **Salva**.

Administration Server riceve gli eventi frequenti sbloccati e non riceve gli eventi frequenti bloccati.

Rimozione del blocco degli eventi frequenti

È possibile rimuovere il blocco per gli eventi frequenti e iniziare a riceverli fino a quando Administration Server bloccherà nuovamente questi eventi frequenti.

Per rimuovere il blocco per gli eventi frequenti:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale**, selezionare la sezione **Blocco degli eventi frequenti**.

3. Nella sezione **Blocco degli eventi frequenti** selezionare i tipi di eventi frequenti per i quali si desidera rimuovere il blocco.

4. Fare clic sul pulsante **Rimuovi il blocco**.

L'evento frequente viene rimosso dall'elenco degli eventi frequenti. Administration Server riceverà gli eventi di questo tipo.

Elaborazione e archiviazione di eventi in Administration Server

Le informazioni sugli eventi che si verificano durante l'esecuzione dell'applicazione e dei dispositivi gestiti vengono salvate nel database di Administration Server. A ogni evento è attribuito un determinato tipo e un livello di criticità (*Evento critico*, *Errore funzionale*, *Avviso* o *informazioni*). A seconda delle condizioni in cui si è verificato un evento, l'applicazione può assegnare diversi livelli di criticità a eventi dello stesso tipo.

È possibile visualizzare i tipi e i livelli di criticità assegnati agli eventi nella sezione **Configurazione eventi** della finestra delle proprietà di Administration Server. Nella sezione **Configurazione eventi** è anche possibile configurare l'elaborazione di ogni evento da parte di Administration Server:

- Registrazione degli eventi in Administration Server e nei registri eventi del sistema operativo in un dispositivo e in Administration Server.

- Metodo utilizzato per notificare un evento all'amministratore (ad esempio, un SMS o un messaggio e-mail).

Nella sezione **Archivio eventi** della finestra delle proprietà di Administration Server è possibile modificare le impostazioni per l'archiviazione degli eventi nel database di Administration Server, limitando il numero di record degli eventi e il periodo di archiviazione dei record. Quando si specifica il numero massimo di eventi, l'applicazione calcola approssimativamente la quantità di spazio di archiviazione necessario per il numero specificato. È possibile utilizzare questo calcolo approssimativo per valutare se è necessario liberare spazio su disco per evitare l'overflow del database. La capacità predefinita del database di Administration Server è di 400.000 eventi. La capacità massima consigliata del database è di 45 milioni di eventi.

L'applicazione controlla il database ogni 10 minuti. Se il numero di eventi raggiunge il valore massimo specificato più 10.000, l'applicazione elimina gli eventi meno recenti in modo che rimanga solo il numero massimo di eventi specificato.

Quando l'Administration Server elimina gli eventi meno recenti, non può salvare i nuovi eventi nel database. Durante questo periodo, le informazioni sugli eventi rifiutati vengono scritte nel registro del sistema operativo. I nuovi eventi vengono accodati e quindi salvati nel database al termine dell'operazione di eliminazione. Per impostazione predefinita, la coda degli eventi è limitata a 20.000 eventi. È possibile personalizzare il limite della coda modificando il valore del contrassegno KLEVP_MAX_POSTPONED_CNT.

Notifiche e stati del dispositivo

Questa sezione contiene informazioni su come visualizzare le notifiche, configurare il recapito delle notifiche, utilizzare gli stati dei dispositivi e abilitare la modifica degli stati dei dispositivi.

Utilizzo delle notifiche

Le notifiche segnalano gli eventi e consentono di velocizzare le risposte a tali eventi eseguendo le azioni consigliate o le azioni che si ritengono appropriate.

A seconda del metodo di notifica scelto, sono disponibili i seguenti tipi di notifiche:

- Notifiche sullo schermo
- Notifiche tramite SMS
- Notifiche tramite e-mail
- Notifiche tramite file eseguibile o script

Notifiche sullo schermo

Le notifiche sullo schermo segnalano gli eventi raggruppati per livelli di importanza (*Critico*, *Avviso* e *Informativo*).

Una notifica sullo schermo può avere due stati:

- *Rivista*. Indica che è stata eseguita l'azione consigliata per la notifica o che è stato assegnato manualmente questo stato per la notifica.
- *Non rivista*. Indica che non è stata eseguita l'azione consigliata per la notifica o che non è stato assegnato manualmente questo stato per la notifica.

Per impostazione predefinita, l'elenco delle notifiche include le notifiche con lo stato *Non rivista*.

È possibile monitorare la rete dell'organizzazione visualizzando le notifiche sullo schermo e rispondendo in tempo reale a tali notifiche.

Notifiche tramite e-mail, SMS e file eseguibile o script

Kaspersky Security Center Linux offre la possibilità di monitorare la rete dell'organizzazione inviando notifiche su qualsiasi evento che si ritiene importante. Per ogni evento è possibile configurare notifiche tramite e-mail, tramite SMS o avviando un file eseguibile o uno script.

Dopo aver ricevuto notifiche tramite e-mail o SMS, è possibile decidere la risposta a un evento. Questa risposta dovrebbe essere la più appropriata per la rete dell'organizzazione. Avviando un file eseguibile o uno script, si specifica una risposta predefinita a un evento. L'avvio di un file eseguibile o di uno script può anche essere considerato la risposta primaria a un evento. Dopo l'avvio del file eseguibile, è possibile eseguire altri passaggi per rispondere all'evento.

Visualizzazione delle notifiche sullo schermo

È possibile visualizzare le notifiche sullo schermo in tre modi:

- Nella sezione **Monitoraggio e generazione dei rapporti** → **Notifiche**. Qui è possibile visualizzare le notifiche relative alle categorie predefinite.
- In una finestra distinta che può essere aperta indipendentemente dalla sezione in uso. In questo caso, è possibile contrassegnare le notifiche come riviste.
- Nel widget **Notifiche in base al livello di criticità selezionato** nella sezione **Monitoraggio e generazione dei rapporti** → **Dashboard**. Nel widget è possibile visualizzare solo le notifiche degli eventi con i livelli di importanza *Critico* e *Avviso*.

È possibile eseguire azioni, ad esempio è possibile rispondere a un evento.

Per visualizzare le notifiche delle categorie predefinite:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Notifiche**.

   La categoria **Tutte le notifiche** è selezionata nel riquadro sinistro e nel riquadro destro sono visualizzate tutte le notifiche.

2. Nel riquadro sinistro selezionare una delle categorie:

   - **Distribuzione**
   - **Dispositivi**
   - **Protezione**
   - **Aggiornamenti** (sono incluse le notifiche relative alle applicazioni Kaspersky disponibili per il download e le notifiche relative agli aggiornamenti dei database anti-virus scaricati)
   - **Prevenzione Exploit**
   - **Administration Server** (sono inclusi gli eventi relativi solo ad Administration Server)
   - **Collegamenti utili** (sono inclusi collegamenti a risorse Kaspersky, ad esempio il Servizio di assistenza tecnica Kaspersky, il forum Kaspersky, la pagina di rinnovo della licenza o Kaspersky IT Encyclopedia)

- **Novità di Kaspersky** (sono incluse le informazioni sulle versioni delle applicazioni Kaspersky)

Viene visualizzato un elenco di notifiche della categoria selezionata. L'elenco contiene i seguenti elementi:

- Icona relativa all'argomento della notifica: distribuzione, protezione, aggiornamenti, gestione dispositivi, Prevenzione Exploit, Administration Server.
- Livello di importanza della notifica. Vengono visualizzate le notifiche con i seguenti livelli di importanza: **Notifiche critiche**, **Notifiche di avviso**, **Notifiche informative**. Le notifiche nell'elenco sono raggruppate in base ai livelli di importanza.
- **Notifica**. Contiene una descrizione della notifica.
- **Azione**. Contiene un collegamento a un'azione rapida che è consigliabile eseguire. Ad esempio, facendo clic su questo collegamento, è possibile passare all'archivio e installare le applicazioni di protezione nei dispositivi oppure visualizzare un elenco di dispositivi o un elenco di eventi. Dopo aver eseguito l'azione consigliata per la notifica, alla notifica viene assegnato lo stato *Rivista*.
- **Stato registrato**. Contiene il numero di giorni o ore trascorsi dal momento in cui la notifica è stata registrata in Administration Server.

Per visualizzare le notifiche sullo schermo in una finestra distinta in base al livello di importanza:

1. Nell'angolo superiore destro di Kaspersky Security Center Web Console, fare clic sull'icona a forma di bandiera ( ).

   Se l'icona a forma di bandiera contiene un punto rosso, sono presenti notifiche che non sono state riviste.

   Verrà visualizzata una finestra che elenca le notifiche. Per impostazione predefinita, la scheda **Tutte le notifiche** è selezionata e le notifiche sono raggruppate per livello di importanza: *Critico*, *Avviso* e *Informazioni*.

2. Selezionare la scheda **Sistema**.

   Verrà visualizzato l'elenco delle notifiche con i livelli di importanza *Critico* e *Avviso*. L'elenco delle notifiche include i seguenti elementi:

   - Contrassegno del colore. Le notifiche critiche sono contrassegnate in rosso. Le notifiche di avviso sono contrassegnate in giallo.
   - Icona che indica l'argomento della notifica: distribuzione, protezione, aggiornamenti, gestione dispositivi, Prevenzione Exploit, Administration Server.
   - Descrizione della notifica.
   - Icona a forma di bandiera. L'icona a forma di bandiera è grigia se alle notifiche è stato assegnato lo stato *Non rivista*. Quando si seleziona l'icona a forma di bandiera di colore grigio e si assegna lo stato *Rivista* a una notifica, il colore dell'icona diventa bianco.
   - Collegamento all'azione consigliata. Quando si esegue l'azione consigliata dopo aver fatto clic sul collegamento, alla notifica viene assegnato lo stato *Rivista*.
   - Numero di giorni trascorsi dalla data in cui la notifica è stata registrata in Administration Server.

3. Selezionare la scheda **Altro**.

   Verrà visualizzato l'elenco delle notifiche con il livello di importanza *Informazioni*.

L'organizzazione dell'elenco è la stessa dell'elenco nella scheda **Sistema** (vedere la descrizione precedente). L'unica differenza è l'assenza di un contrassegno del colore.

È possibile filtrare le notifiche in base all'intervallo di date in cui sono state registrate in Administration Server. Utilizzare la casella di controllo **Mostra filtro** per gestire il filtro.

Per visualizzare le notifiche sullo schermo nel widget:

1. Nella sezione **Dashboard** selezionare **Aggiungi o ripristina widget Web**.
2. Nella finestra visualizzata fare clic sulla categoria **Altro**, selezionare il widget **Notifiche in base al livello di criticità selezionato** e fare clic su Aggiungi.

   Il widget verrà visualizzato nella scheda **Dashboard**. Per impostazione predefinita, nel widget vengono visualizzate le notifiche con il livello di importanza *Critico*.

   È possibile fare clic sul pulsante **Impostazioni** nel widget e modificare le impostazioni del widget per visualizzare le notifiche con il livello di importanza *Avviso*. In alternativa, è possibile aggiungere un altro widget: **Notifiche in base al livello di criticità selezionato**, con un livello di importanza *Avviso*.

   L'elenco delle notifiche nel widget è limitato dalle dimensioni e include due notifiche. Queste due notifiche si riferiscono agli ultimi eventi.

L'elenco delle notifiche nel widget include i seguenti elementi:

- Icona relativa all'argomento della notifica: distribuzione (), protezione (), aggiornamenti (), gestione dispositivi (), Prevenzione Exploit (), Administration Server ().
- Descrizione della notifica con un collegamento all'azione consigliata. Quando si esegue un'azione consigliata dopo aver fatto clic sul collegamento, alla notifica viene assegnato lo stato *Rivista*.
- Numero di giorni o numero di ore trascorsi dalla data in cui la notifica è stata registrata in Administration Server.
- Collegamento ad altre notifiche. Facendo clic su questo collegamento, è possibile passare alla visualizzazione delle notifiche nella sezione **Notifiche** della sezione **Monitoraggio e generazione dei rapporti**.

Informazioni sugli stati dei dispositivi

Kaspersky Security Center Linux assegna uno stato a ciascun dispositivo gestito. Lo stato specifico dipende dal rispetto delle condizioni definite dall'utente. In alcuni casi, durante l'assegnazione di uno stato a un dispositivo, Kaspersky Security Center Linux prende in considerazione il flag di visibilità del dispositivo nella rete (vedere la tabella seguente). Se Kaspersky Security Center Linux non rileva un dispositivo nella rete entro due ore, il flag di visibilità del dispositivo è impostato su *Non visibile*.

Gli stati sono i seguenti:

- *Critico* o *Critico / Visibile*
- *Avviso* o *Avviso / Visibile*
- *OK* o *OK / Visibile*

La tabella seguente elenca le condizioni predefinite da soddisfare per assegnare a un dispositivo lo stato *Critico* o *Avviso*, con tutti i possibili valori.

Condizioni per l'assegnazione di uno stato a un dispositivo

Condizione	Descrizione della condizione	Valori disponibili
Applicazione di protezione non installata	Network Agent è installato nel dispositivo, ma un'applicazione di protezione non è installata.	• L'interruttore è attivato. • L'interruttore è disattivato.
Troppi virus rilevati	Nel dispositivo sono stati rilevati alcuni virus da parte di un'attività per il rilevamento dei virus, ad esempio l'attività Scansione malware, e il numero di virus trovati supera il valore specificato.	Più di 0.
Livello protezione in tempo reale diverso da quello impostato dall'amministratore	Il dispositivo è visibile nella rete, ma il livello della protezione in tempo reale è diverso dal livello impostato (nella condizione) dall'amministratore per lo stato del dispositivo.	• Arrestata. • Sospesa. • In esecuzione.
Scansione malware non eseguita da molto tempo	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma né l'attività *Scansione malware* né un'attività di scansione locale sono state eseguite nell'intervallo di tempo specificato. La condizione è applicabile solo ai dispositivi che sono stati aggiunti al database di Administration Server 7 giorni o più di 7 giorni prima.	Più di 1 giorno.
I database non sono aggiornati	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma i database anti-virus non vengono aggiornati nel dispositivo nell'intervallo di tempo specificato. La condizione è applicabile solo ai dispositivi che sono stati aggiunti al database di Administration Server un giorno o più di un giorno prima.	Più di 1 giorno.
Connessione non eseguita da molto tempo	Network Agent è installato nel dispositivo, ma il dispositivo non viene connesso a un Administration Server nell'intervallo di tempo specificato, perché il dispositivo era spento.	Più di 1 giorno.
Rilevate minacce attive	Il numero di oggetti non elaborati nella cartella **Minacce attive** è superiore al valore specificato.	Più di 0 elementi.
È necessario il riavvio	Il dispositivo è visibile nella rete, ma un'applicazione richiede il riavvio del dispositivo da un periodo superiore all'intervallo di tempo specificato e per uno dei motivi selezionati.	Più di 0 minuti.
Applicazioni incompatibili installate	Il dispositivo è visibile nella rete, ma l'inventario software eseguito tramite Network Agent ha rilevato applicazioni incompatibili installate nel dispositivo.	• L'interruttore è disattivato. • L'interruttore è attivato.
La licenza è scaduta	Il dispositivo è visibile nella rete, ma la licenza è scaduta.	• L'interruttore è disattivato. • L'interruttore è attivato.
La licenza sta per scadere	Il dispositivo è visibile nella rete, ma la licenza nel dispositivo scadrà tra un numero di giorni inferiore rispetto a quello specificato.	Più di 0 giorni.
Stato criptaggio non valido	Network Agent è installato nel dispositivo, ma il risultato del criptaggio dispositivo è uguale al valore specificato.	• Non è conforme al criterio a causa di un rifiuto dell'utente (solo per i dispositivi esterni). • Non è conforme al criterio a causa di un errore. • È richiesto il riavvio per l'applicazione del criterio. • Non è specificato alcun criterio di criptaggio. • Non supportato. • Quando viene applicato il criterio.
Problemi di sicurezza non elaborati rilevati	Sono stati rilevati nel dispositivo alcuni problemi di sicurezza non elaborati. I problemi di sicurezza possono essere creati automaticamente, tramite le applicazioni gestite Kaspersky installate nel dispositivo client, o manualmente, dall'amministratore.	• L'interruttore è disattivato.

		• L'interruttore è attivato.
Stato dispositivo definito dall'applicazione	Lo stato del dispositivo è definito dall'applicazione gestita.	• L'interruttore è disattivato. • L'interruttore è attivato.
Spazio su disco esaurito nel dispositivo	Lo spazio disponibile sul disco nel dispositivo è inferiore al valore specificato o il dispositivo non può essere sincronizzato con Administration Server. Lo stato *Critico* o *Avviso* diventa *OK* quando il dispositivo viene sincronizzato con Administration Server e lo spazio disponibile nel dispositivo è maggiore o uguale al valore specificato.	Più di 0 MB.
Il dispositivo è diventato non gestito	Durante la device discovery, il dispositivo è stato riconosciuto come visibile nella rete, ma più di tre tentativi di sincronizzazione con Administration Server hanno avuto esito negativo.	• L'interruttore è disattivato. • L'interruttore è attivato.
Protezione disattivata	Il dispositivo è visibile nella rete, ma l'applicazione di protezione nel dispositivo è stata disabilitata per un periodo superiore all'intervallo di tempo specificato. In questo caso, lo stato dell'applicazione di protezione è *interrotto* o *non riuscito* e differisce dai seguenti: *avvio*, *esecuzione* o *sospensione*.	Più di 0 minuti.
Applicazione di protezione non in esecuzione	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma non è in esecuzione.	• L'interruttore è disattivato. • L'interruttore è attivato.

Kaspersky Security Center Linux consente di configurare la selezione automatica dello stato di un dispositivo in un gruppo di amministrazione quando vengono soddisfatte le condizioni specificate. Quando vengono soddisfatte le condizioni specificate, al dispositivo client viene assegnato uno dei seguenti stati: *Critico* o *Avviso*. Quando le condizioni specificate non vengono soddisfatte, al dispositivo client viene assegnato lo stato *OK*.

Diversi stati possono corrispondere ai diversi valori di una condizione. Ad esempio, per impostazione predefinita, se alla condizione **I database non sono aggiornati** è associato il valore **Più di 3 giorni**, al dispositivo client sarà assegnato lo stato *Avviso*; se il valore è **Più di 7 giorni**, verrà assegnato lo stato *Critico*.

Se si esegue l'upgrade di Kaspersky Security Center Linux dalla versione precedente, i valori della condizione **I database non sono aggiornati** per l'assegnazione dello stato *Critico* o *Avviso* restano invariati.

Quando Kaspersky Security Center Linux assegna uno stato a un dispositivo, per alcune condizioni (vedere la colonna Descrizione della condizione) viene preso in considerazione il flag di visibilità. Ad esempio, se a un dispositivo gestito è stato assegnato lo stato *Critico* perché è stata soddisfatta la condizione I database non sono aggiornati e successivamente è stato impostato il flag di visibilità per il dispositivo, al dispositivo viene assegnato lo stato *OK*.

Configurazione dell'invio delle notifiche

È possibile configurare notifiche per gli eventi che si verificano in Kaspersky Security Center Linux. A seconda del metodo di notifica scelto, sono disponibili i seguenti tipi di notifiche:

- E-mail: quando si verifica un evento, Kaspersky Security Center Linux invia una notifica agli indirizzi e-mail specificati.
- SMS: quando si verifica un evento, Kaspersky Security Center Linux invia una notifica ai numeri di telefono specificati.

- File eseguibile: quando si verifica un evento, viene eseguito il file eseguibile in Administration Server.

Per configurare l'invio delle notifiche per gli eventi che si verificano in Kaspersky Security Center Linux:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server, con la scheda **Generale** selezionata.

2. Fare clic sulla sezione **Notifica** e nel riquadro destro selezionare la scheda per il metodo di notifica desiderato:

   - **E-mail**

La scheda **E-mail** consente di configurare la notifica degli eventi tramite e-mail.

Nel campo **Server SMTP** specificare gli indirizzi dei server di posta, separandoli con punto e virgola. È possibile utilizzare i seguenti valori:

- Indirizzo IPv4 o IPv6
- Nome DNS del server SMTP

Nel campo **Porta server SMTP** specificare il numero di una porta di comunicazione del server SMTP. Il numero di porta predefinito è 25.

Se si abilita l'opzione **Usa ricerca DNS MX**, è possibile utilizzare più record MX degli indirizzi IP per lo stesso nome DNS del server SMTP. Lo stesso nome DNS può avere diversi record MX con valori di priorità differenti di ricezione dei messaggi e-mail. Administration Server tenta di inviare notifiche e-mail al server SMTP in ordine crescente di priorità dei record MX.

Se si abilita l'opzione **Usa ricerca DNS MX** e non si abilita l'utilizzo delle impostazioni TLS, è consigliabile utilizzare le impostazioni DNSSEC nel dispositivo server come misura di protezione aggiuntiva per l'invio di notifiche e-mail.

Se si abilita l'opzione **Usa autenticazione ESMTP**, è possibile specificare le impostazioni di autenticazione ESMTP nei campi **Nome utente** e **Password**. Per impostazione predefinita, l'opzione è disabilitata e le impostazioni per l'autenticazione ESMTP non sono disponibili.

È possibile specificare le impostazioni di connessione TLS con un server SMTP:

- **Non utilizzare TLS**

È possibile selezionare questa opzione se si desidera disabilitare il criptaggio dei messaggi e-mail.

- **Usa TLS se supportato dal server SMTP**

È possibile selezionare questa opzione se si desidera utilizzare una connessione TLS in un server SMTP. Se il server SMTP non supporta TLS, Administration Server si connette al server SMTP senza utilizzare TLS.

- **Usa sempre TLS, controlla la validità del certificato del server**

È possibile selezionare questa opzione se si desidera utilizzare le impostazioni di autenticazione TLS. Se il server SMTP non supporta TLS, Administration Server non può connettersi al server SMTP.

È consigliabile utilizzare questa opzione per una protezione più efficace della connessione con un server SMTP. Se si seleziona questa opzione, è possibile configurare le impostazioni di autenticazione per una connessione TLS.

Se si seleziona il valore **Usa sempre TLS, controlla la validità del certificato del server**, è possibile specificare un certificato per l'autenticazione del server SMTP e scegliere se si desidera abilitare la comunicazione tramite qualsiasi versione di TLS o solo tramite TLS 1.2 o versioni successive. È inoltre possibile specificare un certificato per l'autenticazione del client nel server SMTP.

È possibile specificare i certificati per una connessione TLS facendo clic sul collegamento **Specifica certificati**:

- Cercare un file di certificato del server SMTP:

È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione attendibile e caricare il file in Administration Server. Kaspersky Security Center Linux verifica se anche il certificato di un server SMTP è firmato da un'autorità di certificazione attendibile. Kaspersky Security Center Linux non può connettersi a un server SMTP se il certificato del server SMTP non viene ricevuto da un'autorità di certificazione attendibile.

- Cercare un file di certificato del client:

È possibile utilizzare un certificato ricevuto da qualsiasi origine, ad esempio da qualsiasi autorità di certificazione attendibile. È necessario specificare il certificato e la relativa chiave privata utilizzando uno dei seguenti tipi di certificato:

- Certificato X-509:

È necessario specificare un file con il certificato e un file con la chiave privata. Entrambi i file non dipendono l'uno dall'altro e l'ordine di caricamento dei file non è significativo. Quando entrambi i file vengono caricati, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

- Contenitore pkcs12:

È necessario caricare un singolo file che contenga il certificato e la relativa chiave privata. Quando il file viene caricato, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

Il pulsante **Invia messaggio di test** consente di verificare se le notifiche sono state configurate correttamente: l'applicazione invia una notifica di prova all'indirizzo e-mail specificato.

Nel campo **Destinatari (indirizzi e-mail)** specificare gli indirizzi e-mail a cui l'applicazione invierà le notifiche. È possibile specificare più indirizzi in questo campo, separandoli con punto e virgola.

Nel campo **Oggetto** specificare l'oggetto del messaggio e-mail. È possibile lasciare vuoto questo campo.

Nell'elenco a discesa **Modello oggetto** selezionare il modello per l'oggetto. Una variabile determinata dal modello selezionato viene automaticamente inserita nel campo **Oggetto**. È possibile creare un oggetto e-mail selezionando diversi modelli di oggetto.

Nel campo **Indirizzo e-mail del mittente: se questa impostazione non è specificata, verrà utilizzato l'indirizzo del destinatario. Avviso: è consigliabile non utilizzare un indirizzo e-mail fittizio** specificare l'indirizzo del mittente del messaggio e-mail. Se si lascia vuoto questo campo, per impostazione predefinita viene utilizzato l'indirizzo del destinatario. Non è consigliabile utilizzare indirizzi e-mail fittizi.

Il campo **Messaggio di notifica** contiene testo standard con le informazioni sull'evento inviate dall'applicazione quando si verifica un evento. Il testo include parametri sostitutivi, ad esempio il nome dell'evento, il nome del dispositivo e il nome di dominio. È possibile modificare il testo del messaggio aggiungendo altri parametri sostitutivi con dettagli più pertinenti sull'evento.

> Se il testo di notifica contiene un segno percentuale (%), è necessario digitarlo due volte di seguito per consentire l'invio del messaggio. Ad esempio, "Il carico della CPU è 100%%".

Il collegamento **Configura un limite numerico per le notifiche** consente di specificare il numero massimo di notifiche che l'applicazione può inviare nell'intervallo di tempo specificato.

- SMS

La scheda **SMS** consente di configurare la trasmissione delle notifiche SMS di diversi eventi a un cellulare. I messaggi SMS vengono inviati tramite un gateway di posta.

Nel campo **Server SMTP** specificare gli indirizzi dei server di posta, separandoli con punto e virgola. È possibile utilizzare i seguenti valori:

- Indirizzo IPv4 o IPv6
- Nome DNS del server SMTP

Nel campo **Porta server SMTP** specificare il numero di una porta di comunicazione del server SMTP. Il numero di porta predefinito è 25.

Se l'opzione **Usa autenticazione ESMTP** è abilitata, è possibile specificare le impostazioni di autenticazione ESMTP nei campi **Nome utente** e **Password**. Per impostazione predefinita, l'opzione è disabilitata e le impostazioni per l'autenticazione ESMTP non sono disponibili.

È possibile specificare le impostazioni di connessione TLS con un server SMTP:

- **Non utilizzare TLS**

È possibile selezionare questa opzione se si desidera disabilitare il criptaggio dei messaggi e-mail.

- **Usa TLS se supportato dal server SMTP**

È possibile selezionare questa opzione se si desidera utilizzare una connessione TLS in un server SMTP. Se il server SMTP non supporta TLS, Administration Server si connette al server SMTP senza utilizzare TLS.

- **Usa sempre TLS, controlla la validità del certificato del server**

È possibile selezionare questa opzione se si desidera utilizzare le impostazioni di autenticazione TLS. Se il server SMTP non supporta TLS, Administration Server non può connettersi al server SMTP.

È consigliabile utilizzare questa opzione per una protezione più efficace della connessione con un server SMTP. Se si seleziona questa opzione, è possibile configurare le impostazioni di autenticazione per una connessione TLS.

Se si seleziona il valore **Usa sempre TLS, controlla la validità del certificato del server**, è possibile specificare un certificato per l'autenticazione del server SMTP e scegliere se si desidera abilitare la comunicazione tramite qualsiasi versione di TLS o solo tramite TLS 1.2 o versioni successive. È inoltre possibile specificare un certificato per l'autenticazione del client nel server SMTP.

È possibile specificare il file del certificato del server SMTP facendo clic sul collegamento **Specifica certificati**. È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione attendibile e caricare il file in Administration Server. Kaspersky Security Center Linux verifica se anche il certificato di un server SMTP è firmato da un'autorità di certificazione attendibile. Kaspersky Security Center Linux non può connettersi a un server SMTP se il certificato del server SMTP non viene ricevuto da un'autorità di certificazione attendibile.

Nel campo **Destinatari (indirizzi e-mail)** specificare gli indirizzi e-mail a cui l'applicazione invierà le notifiche. È possibile specificare più indirizzi in questo campo, separandoli con punto e virgola. Le notifiche verranno inviate ai numeri di telefono associati agli indirizzi e-mail specificati.

Nel campo **Oggetto** specificare l'oggetto del messaggio e-mail.

Nell'elenco a discesa **Modello oggetto** selezionare il modello per l'oggetto. Una variabile basata sul modello selezionato viene inserita nel campo **Oggetto**. È possibile creare un oggetto e-mail selezionando diversi modelli di oggetto.

Nel campo **Indirizzo e-mail del mittente: se questa impostazione non è specificata, verrà utilizzato l'indirizzo del destinatario. Avviso: è consigliabile non utilizzare un indirizzo e-mail fittizio** specificare l'indirizzo del mittente del messaggio e-mail. Se si lascia vuoto questo campo, per impostazione predefinita viene utilizzato l'indirizzo del destinatario. Non è consigliabile utilizzare indirizzi e-mail fittizi.

Nel campo **Numeri di telefono dei destinatari dei messaggi SMS** specificare i numeri di cellulare dei destinatari delle notifiche SMS.

Nel campo **Messaggio di notifica** specificare un testo standard con le informazioni sull'evento inviate dall'applicazione quando si verifica un evento. Il testo può includere parametri sostitutivi, ad esempio il nome dell'evento, il nome del dispositivo e il nome di dominio.

Se il testo di notifica contiene un segno percentuale (%), è necessario digitarlo due volte di seguito per consentire l'invio del messaggio. Ad esempio, "Il carico della CPU è 100%%".

Fare clic su **Invia messaggio di test** per verificare se le notifiche sono state configurate correttamente: l'applicazione invia una notifica di prova al destinatario specificato.

Fare clic sul collegamento **Configura un limite numerico per le notifiche** per specificare il numero massimo di notifiche che l'applicazione può inviare durante l'intervallo di tempo specificato.

- **File eseguibile da avviare**

  Se è selezionato questo metodo di notifica, nel campo di immissione è possibile specificare l'applicazione che verrà avviata quando si verifica un evento.

  Nel campo **File eseguibile da avviare in Administration Server al verificarsi di un evento** specificare la cartella e il nome del file da eseguire. Prima di specificare il file, preparare il file e specificare i segnaposto che definiscono i dettagli dell'evento da inviare nel messaggio di notifica. La cartella e il file specificati devono trovarsi in Administration Server.

  Il collegamento **Configura un limite numerico per le notifiche** consente di specificare il numero massimo di notifiche che l'applicazione può inviare nell'intervallo di tempo specificato.

3. Nella scheda definire le impostazioni di notifica.
4. Fare clic sul pulsante **OK** per chiudere la finestra delle proprietà di Administration Server.

Le impostazioni di invio delle notifiche salvate vengono applicate a tutti gli eventi che si verificano in Kaspersky Security Center Linux.

È possibile sostituire le impostazioni di invio delle notifiche per determinati eventi nella sezione **Configurazione eventi** delle impostazioni di Administration Server, delle impostazioni di un criterio o delle impostazioni di un'applicazione.

Testing delle notifiche

Per verificare l'invio delle notifiche degli eventi, l'applicazione utilizza la notifica di rilevamento del virus di prova EICAR nei dispositivi client.

Per verificare l'invio delle notifiche degli eventi:

1. Arrestare l'attività di protezione del file system in tempo reale in un dispositivo client e copiare il virus di prova EICAR nel dispositivo client. Quindi, abilitare nuovamente la protezione in tempo reale del file system.
2. Eseguire un'attività di scansione per dispositivi client in un gruppo di amministrazione o per dispositivi specifici, compreso uno con il virus di prova EICAR.

   Se l'attività di scansione è configurata correttamente, il virus di prova verrà rilevato. Se le notifiche sono configurate correttamente, si riceverà una notifica del rilevamento di un virus.

Per aprire un record del rilevamento del virus di prova:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.
2. Fare clic sul nome della selezione **Eventi recenti**.

   Nella finestra mostrata, viene visualizzata la notifica del virus di prova.

Il virus di prova EICAR non contiene codice che può danneggiare il dispositivo. Tuttavia, la maggior parte delle applicazioni di protezione identifica il file come un virus. È possibile scaricare il "virus" di prova dal sito Web ufficiale di EICAR.

Notifiche degli eventi visualizzate dall'esecuzione di un file eseguibile

Kaspersky Security Center Linux consente di inviare all'amministratore notifiche degli eventi nei dispositivi client visualizzate dall'esecuzione di un file eseguibile. Il file eseguibile deve contenere un altro file eseguibile con segnaposto dell'evento da inviare all'amministratore (vedere la tabella seguente).

Segnaposto per la descrizione di un evento

Segnaposto	Descrizione del segnaposto
%SEVERITY%	Livello di criticità di un evento. Valori possibili: • **Informazioni** • **Avviso** • **Errore** • **Critico**
%COMPUTER%	Nome del dispositivo in cui si è verificato l'evento. La lunghezza massima del nome del dispositivo è di 256 caratteri.
%DOMAIN%	Nome di dominio del dispositivo in cui si è verificato l'evento
%EVENT%	Nome del tipo di evento. La lunghezza massima del nome del tipo di evento è 50 caratteri.
%DESCR%	Descrizione dell'evento. La lunghezza massima della descrizione è di 1000 caratteri.
%RISE_TIME%	Ora di creazione dell'evento.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nome dell'attività. La lunghezza massima del nome dell'attività è di 100 caratteri.
%KL_PRODUCT%	Nome applicazione.
%KL_VERSION%	Numero di versione dell'applicazione.
%KLCSAK_EVENT_SEVERITY_NUM%	Numero del livello di criticità dell'evento. Valori possibili: • 1—**Informazioni** • 2—**Avviso** • 3—**Errore** • 4—**Critico**
%HOST_IP%	Indirizzo IP del dispositivo in cui si è verificato l'evento.
%HOST_CONN_IP%	Indirizzo IP della connessione del dispositivo in cui si è verificato l'evento.

Esempio:

Le notifiche degli eventi sono inviate tramite un file eseguibile (come script1.bat) all'interno del quale viene avviato un altro file eseguibile (come script2.bat) con il segnaposto %COMPUTER%. Quando si verifica un evento, il file script1.bat viene eseguito nel dispositivo dell'amministratore, eseguendo a sua volta il file script2.bat con il segnaposto %COMPUTER%. L'amministratore riceverà il nome del dispositivo in cui si è verificato l'evento.

Annunci Kaspersky

Questa sezione descrive come utilizzare, configurare e disabilitare gli annunci di Kaspersky.

Informazioni sugli annunci di Kaspersky

La sezione Annunci Kaspersky (**Monitoraggio e generazione dei rapporti → Kaspersky announcements**) consente di rimanere informati fornendo informazioni relative alla versione in uso di Kaspersky Security Center Linux e alle applicazioni gestite installate nei dispositivi gestiti. Kaspersky Security Center Linux aggiorna periodicamente le informazioni nella sezione rimuovendo gli annunci obsoleti e aggiungendo nuove informazioni.

Kaspersky Security Center Linux mostra solo gli annunci di Kaspersky relativi all'Administration Server attualmente connesso e alle applicazioni Kaspersky installate nei dispositivi gestiti di questo Administration Server. Gli annunci vengono visualizzati singolarmente per qualsiasi tipo di Administration Server: primario, secondario o virtuale.

L'Administration Server deve disporre di una connessione Internet per ricevere gli annunci Kaspersky.

Gli annunci includono informazioni dei seguenti tipi:

- Annunci relativi alla sicurezza

  Gli annunci relativi alla sicurezza hanno lo scopo di mantenere aggiornate e completamente funzionanti le applicazioni Kaspersky installate nella rete. Gli annunci possono includere informazioni sugli aggiornamenti critici per le applicazioni Kaspersky, correzioni per le vulnerabilità rilevate e modalità di risoluzione di altri problemi nelle applicazioni Kaspersky. Per impostazione predefinita, gli annunci correlati alla sicurezza sono abilitati. Se non si desidera ricevere gli annunci, è possibile disabilitare questa funzionalità.

  Per mostrare le informazioni corrispondenti alla configurazione della protezione di rete, Kaspersky Security Center Linux invia i dati ai server cloud Kaspersky e riceve solo gli annunci relativi alle applicazioni Kaspersky installate nella rete. Il set di dati che può essere inviato ai server è descritto nel Contratto di licenza con l'utente finale che l'utente accetta durante l'installazione di Kaspersky Security Center Administration Server.

- Annunci di marketing

  Gli annunci di marketing includono informazioni su offerte speciali per le applicazioni Kaspersky, pubblicità e notizie provenienti da Kaspersky. Gli annunci di marketing sono disabilitati per impostazione predefinita. Questo tipo di annunci viene ricevuto solo se è stato abilitato Kaspersky Security Network (KSN). È possibile disabilitare gli annunci di marketing disabilitando KSN.

  Al fine di mostrare solo le informazioni attinenti che potrebbero essere utili per la protezione dei dispositivi di rete e nelle attività quotidiane, Kaspersky Security Center Linux invia i dati ai server cloud Kaspersky e riceve gli annunci appropriati. Il set di dati che può essere inviato ai server è descritto nella sezione Dati elaborati dell' Informativa KSN.

Le nuove informazioni sono suddivise nelle seguenti categorie, in base al livello di importanza:

1. Informazioni critiche
2. Novità importanti

3. Avviso

4. Informazioni

Quando vengono visualizzate nuove informazioni nella sezione Annunci Kaspersky, Kaspersky Security Center Web Console visualizza un'etichetta di notifica che corrisponde al livello di importanza degli annunci. È possibile fare clic sull'etichetta per visualizzare l'annuncio nella sezione Annunci Kaspersky.

È possibile specificare le impostazioni degli annunci Kaspersky, comprese le categorie di annunci che si desidera visualizzare e dove visualizzare l'etichetta di notifica. Se non si desidera ricevere gli annunci, è possibile disabilitare questa funzionalità.

Configurazione delle impostazioni per gli annunci di Kaspersky

Nella sezione Annunci Kaspersky è possibile specificare le impostazioni degli annunci Kaspersky, comprese le categorie di annunci che si desidera visualizzare e dove visualizzare l'etichetta di notifica.

Per configurare gli annunci Kaspersky:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Annunci Kaspersky**.

2. Fare clic sul collegamento **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni degli annunci di Kaspersky.

3. Specificare le seguenti impostazioni:

   - Selezionare il livello di importanza degli annunci che si desidera visualizzare. Gli annunci di altre categorie non verranno visualizzati.

   - Selezionare dove si desidera visualizzare l'etichetta di notifica. L'etichetta può essere visualizzata in tutte le sezioni della console o nella sezione **Monitoraggio e generazione dei rapporti** e nelle relative sottosezioni.

4. Fare clic sul pulsante **OK**.

   Le impostazioni degli annunci Kaspersky sono state specificate.

Disabilitazione degli annunci di Kaspersky

La sezione Annunci Kaspersky (**Monitoraggio e generazione dei rapporti** → **Kaspersky announcements**) consente di rimanere informati fornendo informazioni relative alla versione in uso di Kaspersky Security Center Linux e alle applicazioni gestite installate nei dispositivi gestiti. Se non si desidera ricevere gli annunci di Kaspersky, è possibile disabilitare questa funzionalità.

Gli annunci Kaspersky includono due tipi di informazioni: annunci relativi alla sicurezza e annunci di marketing. È possibile disabilitare separatamente gli annunci di ciascun tipo.

Per disabilitare gli annunci relativi alla sicurezza:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Annunci Kaspersky**.
3. Spostare l'interruttore sulla posizione **Gli annunci relativi alla sicurezza sono disabilitati**.
4. Fare clic sul pulsante **Salva**.

   Gli annunci di Kaspersky vengono disabilitati.

Gli annunci di marketing sono disabilitati per impostazione predefinita. Gli annunci di marketing vengono ricevuti solo se è stato abilitato Kaspersky Security Network (KSN). È possibile disabilitare questo tipo di annunci disabilitando KSN.

Per disabilitare gli annunci di marketing:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN**.
3. Disabilitare l'opzione **Usa Kaspersky Security Network Abilitato**.
4. Fare clic sul pulsante **Salva**.

   Gli annunci di marketing vengono disabilitati.

Esportazione di eventi nei sistemi SIEM

Questa sezione descrive come configurare l'esportazione degli eventi nei sistemi SIEM.

Configurazione dell'esportazione di eventi nei sistemi SIEM

Kaspersky Security Center Linux consente di configurare l'esportazione degli eventi nei sistemi SIEM con uno dei seguenti metodi: esportazione in qualsiasi sistema SIEM che utilizza il formato Syslog o esportazione degli eventi nei sistemi SIEM direttamente dal database di Kaspersky Security Center. Al termine di questo scenario, Administration Server invia automaticamente gli eventi a un sistema SIEM.

Prerequisiti

Prima di avviare la configurazione dell'esportazione degli eventi in Kaspersky Security Center Linux:

- Ulteriori informazioni sui metodi di esportazione degli eventi.
- Assicurarsi di disporre dei valori delle impostazioni di sistema.

> È possibile eseguire i passaggi di questo scenario in qualsiasi ordine.

Il processo di esportazione degli eventi in un sistema SIEM prevede i seguenti passaggi:

- **Configurazione del sistema SIEM per la ricezione di eventi da Kaspersky Security Center Linux**

  Istruzioni dettagliate: Configurazione dell'esportazione di eventi in un sistema SIEM

- **Selezione degli eventi che si desidera esportare nel sistema SIEM**

  Contrassegnare gli eventi da esportare nel sistema SIEM. Innanzitutto, contrassegnare gli eventi generici che si verificano in tutte le applicazioni Kaspersky gestite. Successivamente, è possibile contrassegnare gli eventi per applicazioni Kaspersky gestite specifiche.

- **Configurazione dell'esportazione di eventi nel sistema SIEM**

  Per esportare gli eventi, è possibile utilizzare uno dei seguenti metodi:

  - Utilizzo dei protocolli TCP/IP, UDP o TLS su TCP.
  - Utilizzo dell'esportazione di eventi direttamente dal database di Kaspersky Security Center. È disponibile un set di visualizzazioni pubbliche nel database di Kaspersky Security Center. È possibile trovare la descrizione di queste visualizzazioni pubbliche nel documento klakdb.chm.

Risultati

Dopo aver configurato l'esportazione degli eventi in un sistema SIEM, è possibile visualizzare i risultati dell'esportazione se sono stati selezionati gli eventi da esportare.

Prima di iniziare

Durante la configurazione dell'esportazione automatica degli eventi in Kaspersky Security Center Linux, è necessario specificare alcune impostazioni del sistema SIEM. È consigliabile verificare preventivamente queste impostazioni per la preparazione della configurazione di Kaspersky Security Center Linux.

Per configurare l'invio automatico degli eventi in un sistema SIEM, è necessario conoscere le seguenti impostazioni:

- **Indirizzo server del sistema SIEM**

  L'indirizzo IP del server in cui è installato il sistema SIEM utilizzato attualmente. Verificare questo valore nelle impostazioni del sistema SIEM.

- **Porta server del sistema SIEM**

  Numero della porta utilizzato per stabilire la connessione tra Kaspersky Security Center Linux e il server del sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center Linux e nelle impostazioni del destinatario del sistema SIEM.

- **Protocollo**

  Protocollo utilizzato per il trasferimento dei messaggi da Kaspersky Security Center Linux al sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center Linux e nelle impostazioni del destinatario del sistema SIEM.

Informazioni sull'esportazione degli eventi

Kaspersky Security Center Linux consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Le informazioni sugli eventi vengono salvate nel database di Administration Server.

È possibile utilizzare l'esportazione degli eventi in sistemi centralizzati che gestiscono i problemi di protezione a livello tecnico e organizzativo, garantiscono servizi di monitoraggio della sicurezza e consolidano informazioni da diverse soluzioni. Si tratta di sistemi SIEM, che offrono analisi in tempo reale degli avvisi e degli eventi di protezione generati da applicazioni e hardware di rete o SOC (Security Operation Center).

Questi sistemi ricevono i dati da numerose origini, tra cui reti, sicurezza, server, database e applicazioni. I sistemi SIEM forniscono anche funzionalità per consolidare i dati monitorati ed evitare la perdita di eventi critici. Inoltre, questi sistemi eseguono analisi automatizzate di avvisi ed eventi correlati per inviare immediatamente agli amministratori una notifica dei problemi di protezione. Gli avvisi possono essere implementati tramite un dashboard o inviati tramite canali di terzi, ad esempio via e-mail.

Il processo di esportazione degli eventi da Kaspersky Security Center Linux ai sistemi SIEM esterni coinvolge due parti: un mittente degli eventi, Kaspersky Security Center Linux, e il destinatario di un evento, un sistema SIEM. Per eseguire l'esportazione degli eventi, è necessario configurare questa funzionalità nel sistema SIEM e in Kaspersky Security Center Linux. Non è importante quale lato viene configurato per primo. È possibile configurare la trasmissione degli eventi in Kaspersky Security Center Linux, quindi configurare la ricezione degli eventi dal sistema SIEM o viceversa.

Formato Syslog di esportazione degli eventi

È possibile inviare eventi nel formato Syslog a qualsiasi sistema SIEM. Utilizzando il formato Syslog è possibile inviare gli eventi che si verificano in Administration Server e nelle applicazioni Kaspersky installate nei dispositivi gestiti. Durante l'esportazione degli eventi nel formato Syslog, è possibile selezionare con precisione i tipi di eventi da inviare al sistema SIEM.

Ricezione degli eventi da parte del sistema SIEM

Il sistema SIEM deve ricevere e analizzare correttamente gli eventi ricevuti da Kaspersky Security Center Linux. A tale scopo, è necessario configurare correttamente il sistema SIEM. La configurazione dipende dallo specifico sistema SIEM in uso. Sono comunque previsti diversi passaggi generali per la configurazione di tutti i sistemi SIEM, ad esempio la configurazione del ricevitore e del parser.

Informazioni sulla configurazione dell'esportazione di eventi in un sistema SIEM

Il processo di esportazione degli eventi da Kaspersky Security Center Linux ai sistemi SIEM esterni coinvolge due parti: un mittente degli eventi (Kaspersky Security Center Linux) e il destinatario di un evento (il sistema SIEM). È necessario configurare l'esportazione degli eventi nel sistema SIEM e in Kaspersky Security Center Linux.

Le impostazioni specificate nel sistema SIEM dipendono dal particolare sistema in uso. In genere, per tutti i sistemi SIEM è necessario impostare un ricevitore ed eventualmente un parser dei messaggi per l'analisi degli eventi ricevuti.

Configurazione del ricevitore

Per la ricezione degli eventi inviati da Kaspersky Security Center Linux, è necessario impostare il ricevitore nel sistema SIEM. In generale, le seguenti impostazioni devono essere specificate nel sistema SIEM:

- **Protocollo di esportazione**

  Un protocollo di trasferimento dei messaggi (UDP, TCP o TLS) su TCP. Questo protocollo deve corrispondere al protocollo specificato in Kaspersky Security Center Linux.

- **Porta**

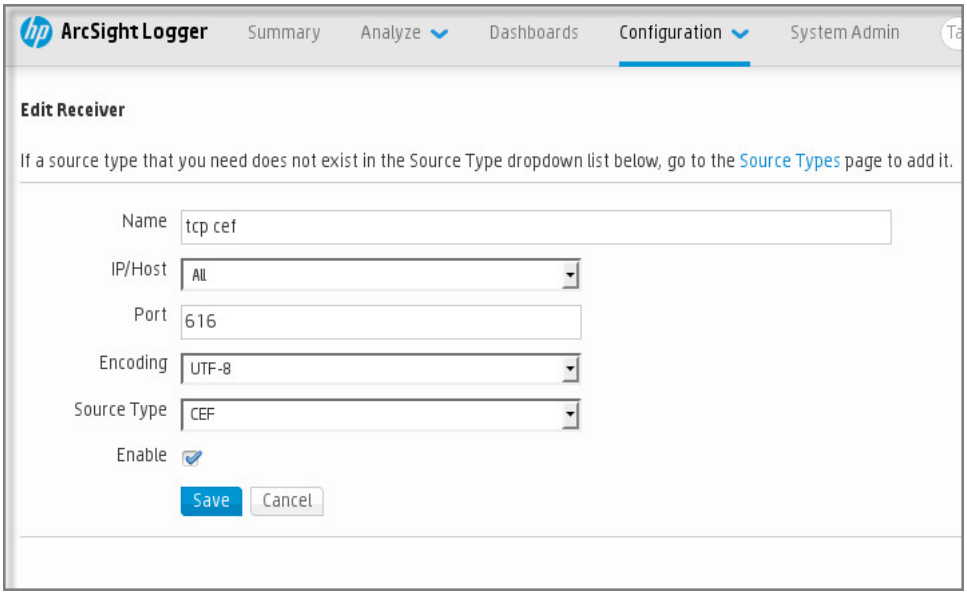
  Specificare il numero di porta per la connessione a Kaspersky Security Center Linux. Deve trattarsi della stessa porta specificata in Kaspersky Security Center Linux durante la configurazione con un sistema SIEM.

- **Formato dei dati**

  Specificare il formato Syslog.

A seconda del sistema SIEM in uso, potrebbe essere necessario specificare alcune impostazioni aggiuntive del ricevitore.

La figura seguente mostra la schermata di configurazione del ricevitore in ArcSight.



Configurazione del ricevitore in ArcSight

Parser dei messaggi

Gli eventi esportati vengono inviati ai sistemi SIEM come messaggi. Questi messaggi devono essere analizzati correttamente per consentire l'utilizzo delle informazioni sugli eventi nel sistema SIEM. I parser dei messaggi fanno parte del sistema SIEM: vengono utilizzati per suddividere il contenuto del messaggio nei campi appropriati, ad esempio l'ID degli eventi, il livello di criticità, la descrizione, i parametri. Questo consente al sistema SIEM di elaborare gli eventi ricevuti da Kaspersky Security Center Linux in modo che possano essere memorizzati nel database del sistema SIEM.

Contrassegno degli eventi per l'esportazione nei sistemi SIEM in formato Syslog

Dopo aver abilitato l'esportazione automatica degli eventi, è necessario selezionare gli eventi da esportare nel sistema SIEM esterno.

È possibile configurare l'esportazione degli eventi in formato Syslog in un sistema esterno in base alle seguenti condizioni:

- Contrassegno di eventi generali. Se si contrassegnano gli eventi da esportare in un criterio, nelle impostazioni di un evento o nelle impostazioni di Administration Server, il sistema SIEM riceverà gli eventi contrassegnati che si sono verificati in tutte le applicazioni gestite dal criterio specifico. Se sono stati selezionati eventi esportati nel criterio, non sarà possibile ridefinirli per una singola applicazione gestita da questo criterio.

- Contrassegno degli eventi per un'applicazione gestita. Se si contrassegnano gli eventi da esportare per un'applicazione gestita installata in un dispositivo gestito, il sistema SIEM riceverà solo gli eventi che si sono verificati nell'applicazione.

Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog

Se si desidera esportare gli eventi che si sono verificati in un'applicazione gestita specifica installata nei dispositivi gestiti, contrassegnare gli eventi per l'esportazione nel criterio dell'applicazione. In questo caso, gli eventi contrassegnati vengono esportati da tutti i dispositivi inclusi nell'ambito del criterio.

Per contrassegnare gli eventi per l'esportazione per una singola applicazione gestita:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio dell'applicazione per cui si desidera contrassegnare gli eventi.

   Verrà visualizzata la finestra delle impostazioni del criterio.
3. Accedere alla sezione **Configurazione eventi**.
4. Selezionare le caselle di controllo accanto agli eventi che si desidera esportare in un sistema SIEM.
5. Fare clic sul pulsante **Contrassegna per l'esportazione nel sistema SIEM utilizzando Syslog**.

   È inoltre possibile contrassegnare un evento per l'esportazione nel sistema SIEM nella sezione **Registrazione eventi** visualizzata facendo clic sul collegamento dell'evento.
6. Un segno di spunta (✓) viene visualizzato nella colonna **Syslog** dell'evento o degli eventi contrassegnati per l'esportazione nel sistema SIEM.
7. Fare clic sul pulsante **Salva**.

Gli eventi contrassegnati dell'applicazione gestita sono pronti per l'esportazione in un sistema SIEM.

È possibile contrassegnare quali eventi esportare in un sistema SIEM per un dispositivo gestito specifico. Se sono stati contrassegnati eventi esportati in precedenza in un criterio dell'applicazione, non sarà possibile ridefinire gli eventi contrassegnati per un singolo dispositivo gestito.

Per contrassegnare gli eventi per l'esportazione per un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Fare clic sul collegamento con il nome del dispositivo desiderato nell'elenco dei dispositivi gestiti.

   Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.

3. Accedere alla sezione **Applicazioni**.

4. Fare clic sul collegamento con il nome dell'applicazione desiderata nell'elenco delle applicazioni.

5. Accedere alla sezione **Configurazione eventi**.

6. Selezionare le caselle di controllo accanto agli eventi che si desidera esportare in SIEM.

7. Fare clic sul pulsante **Contrassegna per l'esportazione nel sistema SIEM utilizzando Syslog**.

   È inoltre possibile contrassegnare un evento per l'esportazione nel sistema SIEM nella sezione **Registrazione eventi** visualizzata facendo clic sul collegamento dell'evento.

8. Un segno di spunta (✓) viene visualizzato nella colonna **Syslog** dell'evento o degli eventi contrassegnati per l'esportazione nel sistema SIEM.

D'ora in poi, Administration Server invia gli eventi contrassegnati al sistema SIEM se è configurata l'esportazione nel sistema SIEM.

Contrassegno di eventi generici per l'esportazione nel formato Syslog

È possibile contrassegnare gli eventi generici che Administration Server esporterà nei sistemi SIEM utilizzando il formato Syslog.

Per contrassegnare eventi generici per l'esportazione in un sistema SIEM:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale, fare clic sull'icona delle impostazioni (🔧) accanto al nome dell'Administration Server richiesto.
   - Nel menu principale, passare a **Risorse (dispositivi)** → **Criteri e profili**, quindi fare clic sul collegamento di un criterio.

2. Nella finestra visualizzata accedere alla scheda **Configurazione eventi**.

3. Fare clic su **Contrassegna per l'esportazione nel sistema SIEM utilizzando Syslog**.

   È inoltre possibile contrassegnare un evento per l'esportazione nel sistema SIEM nella sezione **Registrazione eventi** visualizzata facendo clic sul collegamento dell'evento.

4. Un segno di spunta (✓) viene visualizzato nella colonna **Syslog** dell'evento o degli eventi contrassegnati per l'esportazione nel sistema SIEM.

D'ora in poi, Administration Server invia gli eventi contrassegnati al sistema SIEM se è configurata l'esportazione nel sistema SIEM.

Informazioni sull'esportazione degli eventi utilizzando il formato Syslog

È possibile utilizzare il formato Syslog per esportare nei sistemi SIEM gli eventi che si verificano in Administration Server e in altre applicazioni Kaspersky installate nei dispositivi gestiti.

Syslog è un protocollo standard per la registrazione dei messaggi. Consente una separazione tra il software che genera i messaggi, il sistema che li archivia e il software che li segnala e li analizza. Ogni messaggio dispone di un codice che indica il tipo di software che ha generato il messaggio e di un livello di criticità.

Il formato Syslog è definito dai documenti RFC (Request for Comments) pubblicati da Internet Engineering Task Force (standard Internet). Per l'esportazione degli eventi da Kaspersky Security Center Linux nei sistemi esterni viene utilizzato lo standard RFC 5424.

In Kaspersky Security Center Linux, è possibile configurare l'esportazione degli eventi per i sistemi esterni tramite il formato Syslog.

Il processo di esportazione comprende due passaggi:

1. Abilitazione dell'esportazione automatica degli eventi. In questo passaggio, Kaspersky Security Center Linux viene configurato in modo da inviare gli eventi al sistema SIEM. Kaspersky Security Center Linux inizia a inviare gli eventi subito dopo l'abilitazione dell'esportazione automatica.

2. Selezione degli eventi da esportare nel sistema esterno. In questo passaggio è possibile selezionare gli eventi da esportare nel sistema SIEM.

Configurazione di Kaspersky Security Center Linux per l'esportazione degli eventi nel sistema SIEM

Per esportare gli eventi nel sistema SIEM, è necessario configurare il processo di esportazione in Kaspersky Security Center Linux.

Per configurare l'esportazione nei sistemi SIEM in Kaspersky Security Center Web Console:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale**, selezionare la sezione **SIEM**.

3. Fare clic sul collegamento **Impostazioni**.

   Si aprirà la sezione **Esporta impostazioni**.

4. Specificare le impostazioni nella sezione **Esporta impostazioni**:

   - Indirizzo server del sistema SIEM

L'indirizzo IP del server in cui è installato il sistema SIEM utilizzato attualmente. Verificare questo valore nelle impostazioni del sistema SIEM.

- **Porta del sistema SIEM**

  Numero della porta utilizzato per stabilire la connessione tra Kaspersky Security Center Linux e il server del sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center Linux e nelle impostazioni del destinatario del sistema SIEM.

- **Protocollo**

Selezionare il protocollo da utilizzare per il trasferimento dei messaggi al sistema SIEM. È possibile selezionare il protocollo TCP, UDP o TLS su TCP.

Specificare le seguenti impostazioni TLS se si seleziona il protocollo TLS su TCP:

- **Autenticazione server**

  Nel campo **Autenticazione server**, è possibile selezionare i valori **Certificati affidabili** o **Impronte digitali SHA**:

  - **Certificati affidabili**. È possibile ricevere una catena di certificati completa (incluso il certificato root) da un'autorità di certificazione (CA) attendibile e caricare il file in Kaspersky Security Center Linux. Kaspersky Security Center Linux verifica se anche la catena di certificati del server di sistema SIEM è firmata da un'autorità di certificazione attendibile o meno.

    Per aggiungere un certificato attendibile, fare clic sul pulsante **Cerca il file dei certificati CA**, quindi caricare il certificato.

  - **Impronte digitali SHA**. È possibile specificare le identificazioni personali SHA1 dell'intera catena di certificati del sistema SIEM (incluso il certificato root) in Kaspersky Security Center Linux. Per aggiungere un'identificazione personale SHA1, immetterla nel campo **Identificazioni personali**, quindi fare clic sul pulsante **Aggiungi**.

  Utilizzando l'impostazione **Aggiungi autenticazione client**, è possibile generare un certificato per autenticare Kaspersky Security Center Linux. Pertanto, verrà utilizzato un certificato autofirmato emesso da Kaspersky Security Center Linux. In questo caso, è possibile utilizzare sia un certificato attendibile che un'impronta digitale SHA per autenticare il server di sistema SIEM.

- **Aggiungi nome soggetto/nome alternativo soggetto**

  Il nome del soggetto è un nome di dominio per il quale viene ricevuto il certificato. Kaspersky Security Center Linux non può connettersi al server di sistema SIEM se il nome di dominio del server di sistema SIEM non corrisponde al nome del soggetto del certificato del server di sistema SIEM. Tuttavia, il server di sistema SIEM può modificare il proprio nome di dominio se il nome è stato modificato nel certificato. In questo caso, è possibile specificare i nomi dei soggetti nel campo **Aggiungi nome soggetto/nome alternativo soggetto**. Se uno dei nomi dei soggetti specificati corrisponde al nome del soggetto del certificato di sistema SIEM, Kaspersky Security Center Linux convalida il certificato del server di sistema SIEM.

- **Aggiungi autenticazione client**

  Per l'autenticazione del client, è possibile inserire il certificato o generarlo in Kaspersky Security Center Linux.

  - **Inserire il certificato**. È possibile utilizzare un certificato ricevuto da qualsiasi origine, ad esempio da qualsiasi autorità di certificazione attendibile. È necessario specificare il certificato e la relativa chiave privata utilizzando uno dei seguenti tipi di certificato:

    - **Certificato X.509 PEM**. Caricare un file con un certificato nel campo **File con certificato** e un file con una chiave privata nel campo **File con la chiave**. Entrambi i file non dipendono l'uno dall'altro e l'ordine di caricamento dei file non è significativo. Quando entrambi i file sono stati caricati, specificare la password per la decodifica della chiave privata nel campo **Verifica password o certificato**. La password può avere un valore vuoto se la chiave privata non è codificata.

    - **Certificato X.509 PKCS12**. Caricare un singolo file che contenga un certificato e la relativa chiave privata nel campo **File con certificato**. Quando il file viene caricato, specificare la

password per la decodifica della chiave privata nel campo **Verifica password o certificato**. La password può avere un valore vuoto se la chiave privata non è codificata.

- **Genera chiave**. È possibile generare un certificato autofirmato in Kaspersky Security Center Linux. Di conseguenza, Kaspersky Security Center Linux archivia il certificato autofirmato generato ed è possibile passare la parte pubblica del certificato o l'impronta digitale SHA1 al sistema SIEM.

5. Facoltativamente è possibile esportare gli eventi archiviati dal database di Administration Server e impostare la data di inizio da cui si desidera avviare l'esportazione degli eventi archiviati:
   a. Fare clic sul collegamento **Impostare la data di inizio dell'esportazione**.
   b. Nella sezione visualizzata specificare la data di inizio nel campo **Data da cui iniziare l'esportazione**.
   c. Fare clic sul pulsante **OK**.
6. Spostare l'opzione sulla posizione **Esporta automaticamente gli eventi nel database del sistema SIEM Abilitato**.
7. Fare clic sul pulsante **Salva**.

L'esportazione nel sistema SIEM è configurata. D'ora in poi, se è stata configurata la ricezione degli eventi in un sistema SIEM, Administration Server esporta gli eventi contrassegnati in un sistema SIEM. Se si imposta la data di inizio dell'esportazione, Administration Server esporta anche gli eventi contrassegnati archiviati nel database di Administration Server dalla data specificata.

Esportazione degli eventi direttamente dal database

È possibile recuperare gli eventi direttamente dal database di Kaspersky Security Center Linux senza dover utilizzare l'interfaccia di Kaspersky Security Center Linux. È possibile eseguire direttamente le query sulle visualizzazioni pubbliche e recuperare i dati degli eventi o creare le proprie visualizzazioni sulla base delle visualizzazioni pubbliche esistenti e configurarle in modo che recuperino i dati necessari.

Visualizzazioni pubbliche

Per maggiore praticità, è disponibile un set di visualizzazioni pubbliche nel database di Kaspersky Security Center Linux. È possibile trovare la descrizione di queste visualizzazioni pubbliche nel documento klakdb.chm.

La visualizzazione pubblica v_akpub_ev_event contiene un set di campi che rappresentano i parametri degli eventi nel database. Nel documento klakdb.chm è inoltre possibile trovare informazioni sulle visualizzazioni pubbliche che corrispondono ad altre entità di Kaspersky Security Center Linux, ad esempio dispositivi, applicazioni o utenti. È possibile utilizzare queste informazioni nelle query.

Questa sezione contiene le istruzioni per l'esecuzione di una query SQL tramite l'utilità klsql2 e un esempio di query.

Per creare query SQL o visualizzazioni di database, è anche possibile utilizzare qualsiasi altro programma per l'utilizzo dei database. Le informazioni su come visualizzare i parametri per la connessione al database di Kaspersky Security Center Linux, ad esempio il nome istanza e il nome database, sono indicate nella sezione corrispondente.

Esecuzione di una query SQL tramite l'utilità klsql2

Questo articolo descrive come utilizzare l'utilità klsql2 e come eseguire una query SQL utilizzando questa utilità. Utilizzare la versione dell'utilità klsql2 inclusa nella versione di Kaspersky Security Center Linux installata.

Per utilizzare l'utilità klsql2:

1. Accedere alla directory in cui è installato Administration Server. Il percorso di installazione predefinito è /opt/kaspersky/ksc64/sbin.
2. In questa directory, creare un file vuoto con estensione .sql.
3. Aprire il file .sql creato in qualsiasi editor di testo.
4. Nel file .sql digitare la query SQL desiderata e salvare il file.
5. Nel dispositivo in cui è installato Administration Server digitare nella riga di comando il seguente comando per eseguire la query SQL dal file .sql e salvare i risultati nel file result.xml:
   ```
   sudo ./klsql2 -i src.sql -u <nome utente> -p <password> -o result.xml
   ```
   dove <nome utente> e <password> sono le credenziali dell'account utente che ha accesso al database.
6. Se richiesto, inserire account utente e password dell'account utente che ha accesso al database.
7. Aprire i file result.xml creati per visualizzare i risultati della query SQL.

È possibile modificare il file .sql e creare qualsiasi query SQL sulle visualizzazioni pubbliche. Eseguire la query dalla riga di comando e salvare i risultati in un file.

Esempio di una query SQL nell'utilità klsql2

Questa sezione fornisce un esempio di query SQL, eseguita tramite l'utilità klsql2.

I seguenti esempi illustrano il recupero degli eventi che si sono verificati nei dispositivi negli ultimi sette giorni e la visualizzazione degli eventi ordinati in base all'ora in cui si sono verificati. Gli eventi più recenti vengono visualizzati per primi.

Esempio per PostgreSQL:

```
SELECT
  /* identificatore dell'evento */
  "e"."nId",

  /* ora in cui si è verificato l'evento */
  "e"."tmRiseTime",

  /* nome interno del tipo di eventoe */
  "e"."strEventType",

  /* nome visualizzato dell'evento */
  "e"."wstrEventTypeDisplayName",

  /* descrizione visualizzata dell'evento */
  "e"."wstrDescription",

  /* descrizione visualizzata dell'evento */
  "e"."wstrGroupName",
```

```
    /* nome visualizzato del dispositivo in cui si è verificato l'evento */
    "h"."wstrDisplayName",
    (
      CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
      CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
      CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

      /* indirizzo IP del dispositivo, in cui si è verificato l'evento */
      CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
    )  AS "strIp"
  FROM "v_akpub_ev_event"  AS "e"
    INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
  WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
  ORDER BY "e"."tmRiseTime" DESC ;
```

Esempio per MySQL o MariaDB:

```
  SELECT

    /* identificatore dell'evento */
    `e`.`nId`,

    /* ora in cui si è verificato l'evento */
    `e`.`tmRiseTime`,

    /* nome interno del tipo di eventoe */
    `e`.`strEventType`,

    /* nome visualizzato dell'evento */
    `e`.`wstrEventTypeDisplayName`,

    /* descrizione visualizzata dell'evento */
    `e`.`wstrDescription`,

    /* nome del gruppo di dispositivi */
    `e`.`wstrGroupName`,

    /* nome visualizzato del dispositivo in cui si è verificato l'evento */
    `h`.`wstrDisplayName`,
    CONCAT(
      LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
      LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
      LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

      /* indirizzo IP del dispositivo, in cui si è verificato l'evento */
      LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
    )  AS `strIp`
  FROM `v_akpub_ev_event`  AS `e`
    INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
  WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
  ORDER BY `e`.`tmRiseTime` DESC ;
```

Visualizzazione del nome del database di Kaspersky Security Center Linux

Se si desidera accedere al database di Kaspersky Security Center Linux tramite gli strumenti di gestione database MySQL o MariaDB, è necessario conoscere il nome del database per connettersi dall'editor degli script SQL.

Per visualizzare il nome del database di Kaspersky Security Center Linux:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale**, selezionare la sezione **Dettagli del database corrente**.

Il nome del database è specificato nel campo **Nome database**. Utilizzare il nome del database per fare riferimento al database nelle query SQL.

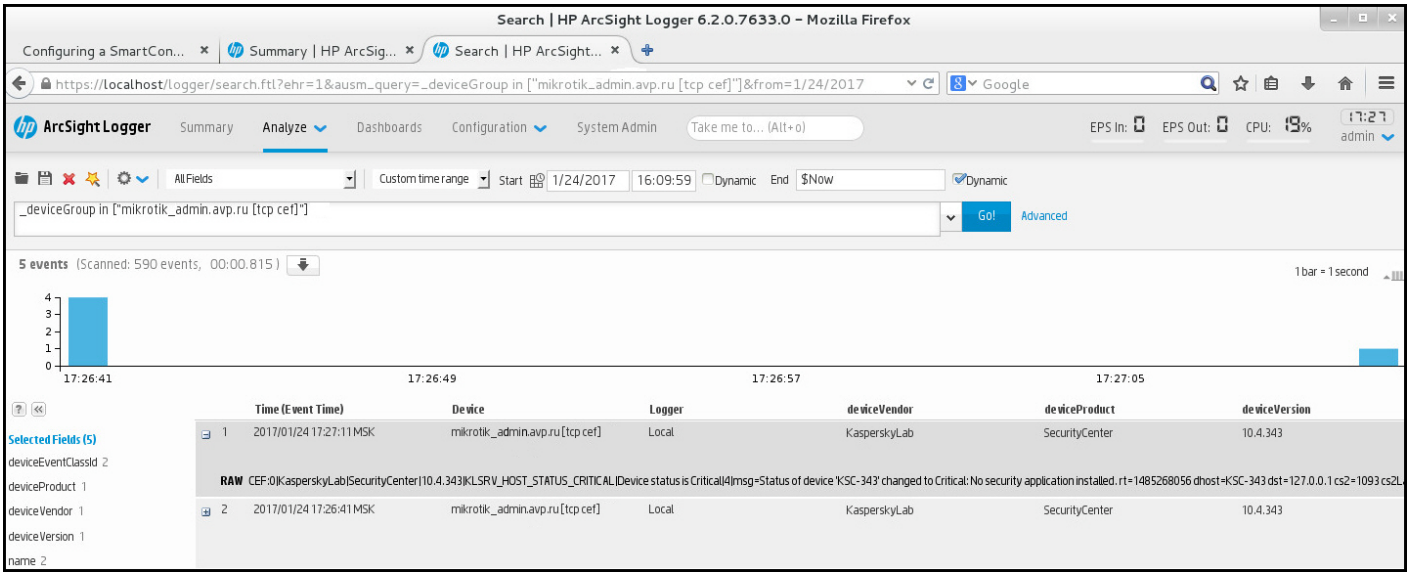
Visualizzazione dei risultati dell'esportazione

È possibile controllare il completamento della procedura di esportazione degli eventi. A tale scopo, controllare se i messaggi con gli eventi esportati vengono ricevuti dal sistema SIEM.

Se gli eventi inviati da Kaspersky Security Center Linux vengono ricevuti e analizzati correttamente dal sistema SIEM, la configurazione su entrambi i lati è stata eseguita correttamente. In caso contrario, controllare le impostazioni specificate in Kaspersky Security Center Linux rispetto alla configurazione del sistema SIEM.

La figura seguente illustra gli eventi esportati in ArcSight. Ad esempio, il primo evento è un evento critico di Administration Server: "*Lo stato del dispositivo è Critico*".

La rappresentazione degli eventi esportati nel sistema SIEM varia in base al sistema SIEM in uso.



Esempio di eventi

Gestione delle revisioni degli oggetti

Questa sezione contiene informazioni sulla gestione delle revisioni degli oggetti. Kaspersky Security Center Linux consente di tenere traccia delle modifiche apportate agli oggetti. Ogni volta che si salvano le modifiche apportate a un oggetto, viene creata una *revisione*. Ogni revisione ha un numero.

Gli oggetti delle applicazioni che supportano la gestione delle revisioni includono:

- Proprietà di Administration Server
- Criteri
- Attività
- Gruppi di amministrazione
- Account utente
- Pacchetti di installazione

È possibile visualizzare l'elenco delle revisioni ed eseguire il rollback delle modifiche apportate a un oggetto in una revisione selezionata.

Nella finestra delle proprietà di un oggetto che supporta la gestione delle revisioni, la sezione **Cronologia revisioni** visualizza un elenco delle revisioni degli oggetti con i seguenti dettagli:

- **Revisione**—Numero di revisione dell'oggetto.
- **Data/ora**—Data e ora di modifica dell'oggetto.
- **Utente**—Nome dell'utente che ha modificato l'oggetto.
- **Azione**—Azione eseguita sull'oggetto.
- **Descrizione**—Descrizione della revisione relativa alla modifica apportata alle impostazioni dell'oggetto.

  Per impostazione predefinita, la descrizione della revisione dell'oggetto è vuota. Per aggiungere una descrizione a una revisione, selezionare la revisione desiderata, quindi fare clic sul pulsante **Modifica descrizione**. Nella finestra aperta, immettere il testo relativo alla descrizione della revisione.

Rollback di un oggetto a una revisione precedente

È possibile eseguire il rollback delle modifiche apportate a un oggetto, se necessario. Potrebbe ad esempio essere necessario ripristinare lo stato delle impostazioni di un criterio in una data specifica.

Per eseguire il rollback delle modifiche apportate a un oggetto:

1. Nella finestra delle proprietà dell'oggetto aprire la scheda **Cronologia revisioni**.
2. Nell'elenco delle revisioni dell'oggetto selezionare la revisione per la quale si desidera eseguire il rollback delle modifiche.
3. Fare clic sul pulsante **Rollback**.
4. Fare clic su **OK** per confermare l'operazione.

   Verrà eseguito il rollback dell'oggetto alla revisione selezionata. L'elenco delle revisioni dell'oggetto visualizza un record dell'azione eseguita. La descrizione della revisione indica il numero della revisione a cui è stato riportato l'oggetto.

L'operazione di rollback è disponibile solo per gli oggetti delle attività e dei criteri.

Eliminazione di oggetti

Questa sezione fornisce informazioni sull'eliminazione degli oggetti.

È possibile eliminare oggetti come:

- Criteri

- Attività
- Pacchetti di installazione
- Administration Server virtuali
- Utenti
- Gruppi di protezione
- Gruppi di amministrazione

Per eliminare un oggetto:

1. Aprire la sezione richiesta di Kaspersky Security Center Web Console, quindi selezionare l'oggetto.
2. Nella barra degli strumenti, fare clic sul pulsante **Elimina**.
3. Nella finestra visualizzata fare clic su **OK** per confermare la selezione.

L'oggetto selezionato verrà eliminato.

Quando si elimina un oggetto, le relative informazioni rimangono nel database. Il periodo di archiviazione per le informazioni sugli oggetti eliminati corrisponde al periodo di archiviazione per le revisioni degli oggetti (il periodo consigliato è di 90 giorni). È possibile modificare il periodo di archiviazione solo se si dispone dell'autorizzazione **Modifica** nell'area dei diritti **Oggetti eliminati**.

Informazioni sull'eliminazione dei dispositivi client

Quando si elimina un dispositivo gestito da un gruppo di amministrazione, l'applicazione sposta il dispositivo nel gruppo Dispositivi non assegnati. Dopo l'eliminazione del dispositivo, le applicazioni Kaspersky installate, Network Agent e qualsiasi applicazione di protezione, ad esempio Kaspersky Endpoint Security, rimangono nel dispositivo.

Kaspersky Security Center Linux gestisce i dispositivi nel gruppo Dispositivi non assegnati in base alle seguenti regole:

- Se sono state configurate regole di spostamento dei dispositivi e un dispositivo soddisfa i criteri di una regola di spostamento, il dispositivo viene spostato automaticamente in un gruppo di amministrazione in base alla regola.
- Il dispositivo viene archiviato nel gruppo Dispositivi non assegnati e rimosso automaticamente dal gruppo in base alle regole di conservazione dei dispositivi.

  Le regole di conservazione dei dispositivi non influiscono sui dispositivi con una o più unità criptate con Criptaggio dell'intero disco. Tali dispositivi non vengono eliminati automaticamente; è possibile eliminarli solo manualmente. Se è necessario eliminare un dispositivo con un'unità criptata, decriptare prima l'unità, quindi eliminare il dispositivo.

  Quando si elimina un dispositivo con un'unità criptata, vengono eliminati anche i dati necessari per decriptare l'unità. Se si seleziona la casella di controllo **Comprendo il rischio e desidero eliminare i dispositivi selezionati** nella finestra di conferma che si apre quando si eliminano tali dispositivi (dal gruppo **Dispositivi non assegnati** o **Dispositivi gestiti**), significa che si è a conoscenza della successiva eliminazione dei dati.

Per decriptare l'unità, devono essere soddisfatte le seguenti condizioni:

- Il dispositivo viene riconnesso ad Administration Server al fine di ripristinare i dati necessari per decriptare l'unità.
- L'utente del dispositivo ricorda la password di decriptaggio.
- L'applicazione di protezione utilizzata per criptare l'unità, ad esempio Kaspersky Endpoint Security for Windows, è ancora installata nel dispositivo.

Se l'unità è stata criptata con la tecnologia Criptaggio disco Kaspersky, è inoltre possibile provare a recuperare i dati utilizzando l'utilità di ripristino FDERT.

Quando si elimina manualmente un dispositivo dal gruppo Dispositivi non assegnati, l'applicazione rimuove il dispositivo dall'elenco. Dopo l'eliminazione del dispositivo, le eventuali applicazioni Kaspersky installate rimangono nel dispositivo. Quindi, se il dispositivo è ancora visibile in Administration Server ed è stato configurato il polling di rete periodico, Kaspersky Security Center Linux rileva il dispositivo durante il polling di rete e lo aggiunge nuovamente al gruppo Dispositivi non assegnati. Pertanto, è ragionevole eliminare manualmente un dispositivo solo se il dispositivo è invisibile ad Administration Server.

Download ed eliminazione dei file da Quarantena e Backup

Questa sezione fornisce informazioni su come scaricare ed eliminare file da Quarantena e Backup in Kaspersky Security Center Web Console.

Download dei file da Quarantena e Backup

È possibile scaricare i file da Quarantena e Backup solo se viene soddisfatta una delle due condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Per salvare una copia del file dalla cartella Quarantena o Backup sul disco rigido:

1. Eseguire una delle seguenti operazioni:
   - Se si desidera salvare una copia del file dalla Quarantena, nel menu principale passare a **Operazioni** → **Archivi** → **Quarantena**.
   - Se si desidera salvare una copia del file da Backup, nel menu principale passare a **Operazioni** → **Archivi** → **Backup**.
2. Nella finestra visualizzata selezionare un file che si desidera scaricare e fare clic su **Scarica**.

Il download viene avviato. Una copia del file che era stato inserito in Quarantena nel dispositivo client viene salvata nella cartella specificata.

Informazioni sulla rimozione di oggetti dagli archivi Quarantena, Backup o Minacce attive

Quando le applicazioni di protezione Kaspersky installate nei dispositivi client inseriscono oggetti negli archivi Quarantena, Backup o Minacce attive, inviano le informazioni sugli oggetti aggiunti alle sezioni **Quarantena**, **Backup**, or **Minacce attive** in Kaspersky Security Center Linux. Quando viene aperta una di queste sezioni, si seleziona un oggetto nell'elenco e si fa clic sul pulsante **Rimuovi**, Kaspersky Security Center Linux esegue una delle seguenti azioni o entrambe le azioni:

- Rimuove l'oggetto selezionato dall'elenco
- Elimina l'oggetto selezionato dall'archivio

L'azione da eseguire è definita dall'applicazione Kaspersky che ha inserito l'oggetto selezionato nell'archivio. L'applicazione Kaspersky è specificata nel campo **Voce aggiunta da**. Fare riferimento alla documentazione dell'applicazione Kaspersky per i dettagli sull'azione da eseguire.

Diagnostica remota dei dispositivi client

È possibile utilizzare la diagnostica remota per l'esecuzione remota delle seguenti operazioni nei dispositivi client basati su Windows e basati su Linux:

- Abilitazione e disabilitazione del tracciamento, modifica del livello di traccia e download del file di traccia
- Download di informazioni sul sistema e impostazioni dell'applicazione
- Download dei registri eventi
- Generazione di un file di dump per un'applicazione
- Avvio della diagnostica e download dei rapporti
- Avvio, arresto e riavvio delle applicazioni

È possibile utilizzare i registri eventi e i rapporti di diagnostica scaricati da un dispositivo client per eseguire autonomamente la risoluzione dei problemi. Inoltre, se si contatta il Servizio di assistenza tecnica Kaspersky, uno specialista del Servizio di assistenza tecnica potrebbe richiedere di scaricare file di traccia, file di dump, registri eventi e rapporti di diagnostica da un dispositivo client per ulteriori analisi da parte di Kaspersky.

Apertura della finestra di diagnostica remota

Per eseguire la diagnostica remota in dispositivi client basati su Windows e basati su Linux, è prima necessario aprire la finestra di diagnostica remota.

Per aprire la finestra di diagnostica remota:

1. Per selezionare il dispositivo per cui si desidera aprire la finestra di diagnostica remota, eseguire una delle seguenti operazioni:
   - Se il dispositivo appartiene a un gruppo di amministrazione, nel menu principale passare a **Risorse (dispositivi)** → **Dispositivi gestiti**.
   - Se il dispositivo appartiene al gruppo Dispositivi non assegnati, nel menu principale passare a **Individuazione e distribuzione** → **Dispositivi non assegnati**.
2. Fare clic sul nome del dispositivo desiderato.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Avanzate**.
4. Nella finestra visualizzata fare clic su **Diagnostica remota**.

   Viene aperta la finestra **Diagnostica remota** di un dispositivo client. Se la connessione tra Administration Server e il dispositivo client non viene stabilita, viene visualizzato il messaggio di errore.

In alternativa, se è necessario ottenere tutte le informazioni diagnostiche su un dispositivo client basato su Linux, è possibile eseguire lo script collect.sh in questo dispositivo.

Abilitazione e disabilitazione del tracciamento per le applicazioni

È possibile abilitare e disabilitare il tracciamento per le applicazioni, incluso il tracciamento Xperf.

Abilitazione e disabilitazione del tracciamento

Per abilitare o disabilitare il tracciamento in un dispositivo remoto:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni, selezionare l'applicazione per cui si desidera disabilitare il tracciamento.

   Si apre l'elenco delle opzioni di diagnostica remota.
4. Se si desidera abilitare il tracciamento:

   a. Nella sezione **Traccia**, fare clic su **Abilita traccia**.

   b. Nella finestra **Modifica livello di traccia** visualizzata è consigliabile mantenere i valori predefiniti delle impostazioni. Se necessario, uno specialista del Servizio di assistenza tecnica fornirà il supporto richiesto per il processo di configurazione. Sono disponibili le seguenti impostazioni:

   - **Livello di traccia**

     Il livello di traccia definisce la quantità di dettagli contenuti nel file di traccia.

   - **Traccia basata sulla rotazione**

     L'applicazione sovrascrive le informazioni di tracciamento per evitare un aumento eccessivo delle dimensioni del file di traccia. Specificare il numero massimo di file da utilizzare per archiviare le informazioni di tracciamento e la dimensione massima di ciascun file. Se viene eseguita la scrittura del numero massimo di file di traccia della dimensione massima, il file di traccia meno recente viene eliminato in modo da consentire la creazione di un nuovo file di traccia.

     Questa impostazione è disponibile solo per Kaspersky Endpoint Security.

   c. Fare clic su **Salva**.

   Il tracciamento è abilitato per l'applicazione selezionata. In alcuni casi, è necessario riavviare un'applicazione di protezione e la relativa attività per abilitare il tracciamento.

   Nei dispositivi client basati su Linux, il tracciamento per il componente Updater of Network Agent è regolata dalle impostazioni di Network Agent. Pertanto, le opzioni **Abilita traccia** e **Modifica livello di traccia** sono disabilitate per questo componente nei dispositivi client in cui viene eseguito Linux.
5. Se si desidera disabilitare il tracciamento per l'applicazione selezionata, fare clic sul pulsante **Disabilita traccia**.

   Il tracciamento è disabilitato per l'applicazione selezionata.

Abilitazione del tracciamento Xperf

Per Kaspersky Endpoint Security, uno specialista del Servizio di assistenza tecnica può richiedere di abilitare il tracciamento Xperf per ottenere informazioni sulle prestazioni del sistema.

Per abilitare e configurare il tracciamento Xperf o disabilitarlo:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni selezionare Kaspersky Endpoint Security for Windows.

   Viene visualizzato l'elenco delle opzioni di diagnostica remota per Kaspersky Endpoint Security for Windows.
4. Nella sezione **Traccia Xperf**, fare clic su **Abilita traccia Xperf**.

   Se il tracciamento Xperf è già abilitato, viene invece visualizzato il pulsante **Disabilita traccia Xperf**. Fare clic su questo pulsante se si desidera disabilitare il tracciamento Xperf per Kaspersky Endpoint Security for Windows.
5. Nella finestra **Modifica livello di traccia Xperf** visualizzata, a seconda di quanto richiesto dallo specialista del Servizio di assistenza tecnica, eseguire una delle seguenti azioni:

   a. Selezionare uno dei seguenti livelli di traccia:

   - **Livello superficiale**

     Un file di traccia di questo tipo contiene la quantità minima di informazioni sul sistema.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Livello approfondito**

     Un file di traccia di questo tipo contiene informazioni più dettagliate rispetto ai file di traccia di tipo *Superficiale* e può essere richiesto dagli specialisti del Servizio di assistenza tecnica quando un file di traccia di tipo *Superficiale* non è sufficiente per la valutazione delle prestazioni. Un file di traccia *Approfondito* contiene informazioni tecniche sul sistema, incluse informazioni su hardware, sistema operativo, elenco di processi e applicazioni avviati e arrestati, eventi utilizzati per la valutazione delle prestazioni ed eventi raccolti da Strumento Valutazione sistema Windows.

   b. Selezionare uno dei seguenti tipi di tracciamento Xperf:

   - **Tipologia di base**

     Le informazioni di tracciamento vengono ricevute durante l'esecuzione dell'applicazione Kaspersky Endpoint Security.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Tipologia al riavvio**

     Le informazioni di tracciamento vengono ricevute all'avvio del sistema operativo nel dispositivo gestito. Questo tipo di tracciamento è utile quando il problema che influisce sulle prestazioni del sistema si verifica dopo l'accensione del dispositivo e prima dell'avvio di Kaspersky Endpoint Security.

Potrebbe anche essere necessario abilitare l'opzione **Dimensioni del file con rotazione (MB)** per impedire un aumento eccessivo delle dimensioni del file di traccia. Specificare quindi la dimensione massima del file di traccia. Quando il file raggiunge la dimensione massima, le informazioni di tracciamento meno recenti vengono sovrascritte da quelle nuove.

c. Definire le dimensioni del file di rotazione.

d. Fare clic su **Salva**.

Il tracciamento Xperf è abilitato e configurato.

6. Se si desidera disabilitare il tracciamento Xperf per Kaspersky Endpoint Security for Windows, fare clic su **Disabilita traccia Xperf** nella sezione **Traccia Xperf**.

   Il tracciamento Xperf è disabilitato.

Download dei file di traccia di un'applicazione

Per scaricare un file di traccia di un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni, selezionare l'applicazione per la quale si desidera scaricare un file di traccia.
4. Nella sezione **Traccia** fare clic sul pulsante **File di traccia**.

   Viene aperta la finestra **Log di traccia del dispositivo**, dove viene visualizzato un elenco dei file di traccia.
5. Nell'elenco dei file di traccia, selezionare il file che si desidera scaricare.
6. Eseguire una delle seguenti operazioni:

   - Scaricare il file selezionato facendo clic su **Scarica**. È possibile selezionare uno o più file da scaricare.
   - Scaricare una parte del file selezionato:

     a. Fare clic su **Scarica una parte**.

     Non è possibile scaricare parti di più file contemporaneamente. Se si seleziona più di un file di traccia, il pulsante **Scarica una parte** sarà disabilitato.

     b. Nella finestra visualizzata specificare il nome e la parte del file da scaricare, in base alle esigenze.

     Per i dispositivi basati su Linux, la modifica del nome di parte del file non è disponibile.

     c. Fare clic su **Scarica**.

Il file selezionato, o la relativa parte, viene scaricato nella posizione specificata.

Eliminazione dei file di traccia

È possibile eliminare i file di traccia non più necessari.

Per eliminare un file di traccia:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra di diagnostica remota visualizzata, selezionare la scheda **Log eventi**.
3. Nella sezione **File di traccia**, fare clic su **Log di Windows Update** o **Log di installazione remota**, in base ai file di traccia che si desidera eliminare.

   Il collegamento ai **Log di Windows Update** è disponibile solo per i dispositivi client basati su Windows.

   Viene aperta la finestra **Log di traccia del dispositivo**, dove viene visualizzato un elenco dei file di traccia.
4. Nell'elenco dei file di traccia, selezionare uno o più file da eliminare.
5. Fare clic sul pulsante **Rimuovi**.

I file di traccia selezionati vengono eliminati.

Download delle impostazioni delle applicazioni

Per scaricare le impostazioni dell'applicazione da un dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.
3. Nella sezione **Impostazioni applicazione**. fare clic sul pulsante **Scarica** per scaricare le informazioni sulle impostazioni delle applicazioni installate nel dispositivo client.

L'archivio ZIP con le informazioni viene scaricato nella posizione specificata.

Download delle informazioni di sistema da un dispositivo client

Per scaricare le informazioni di sistema da un dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Informazioni di sistema**.
3. Fare clic sul pulsante **Scarica** per scaricare le informazioni di sistema sul dispositivo client.

   Se si ottengono informazioni di sistema su un dispositivo basato su Linux, al file risultante viene aggiunto un file di dump per le applicazioni con terminazione di emergenza.

Il file con le informazioni viene scaricato nella posizione specificata.

Download dei registri eventi

Per scaricare un registro eventi da un dispositivo remoto:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, nella scheda **Log eventi**, fare clic su **Tutti i log del dispositivo**.
3. Nella finestra **Tutti i log del dispositivo**, selezionare uno o più log pertinenti.
4. Eseguire una delle seguenti operazioni:
   - Scaricare il log selezionato facendo clic su **Scarica l'intero file**.
   - Scaricare una parte del log selezionato:
     a. Fare clic su **Scarica una parte**.
        Non è possibile scaricare parti di più registri contemporaneamente. Se si seleziona più di un registro eventi, il pulsante **Scarica una parte** sarà disabilitato.
     b. Nella finestra visualizzata specificare il nome e la parte del registro da scaricare, in base alle esigenze.
        Per i dispositivi basati su Linux, la modifica del nome di parte del registro non è disponibile.
     c. Fare clic su **Scarica**.

Il registro eventi selezionato, o la relativa parte, viene scaricato nella posizione specificata.

Avvio, arresto, riavvio dell'applicazione

È possibile avviare, arrestare e riavviare le applicazioni in un dispositivo client.

Per avviare, arrestare o riavviare un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.
   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni selezionare l'applicazione che si desidera avviare, arrestare o riavviare.
4. Selezionare un'azione facendo clic su uno dei seguenti pulsanti:
   - **Arresta applicazione**
     Questo pulsante è disponibile solo se l'applicazione è attualmente in esecuzione.
   - **Riavvia applicazione**
     Questo pulsante è disponibile solo se l'applicazione è attualmente in esecuzione.
   - **Avvia applicazione**

Questo pulsante è disponibile solo se l'applicazione non è attualmente in esecuzione.

A seconda dell'azione selezionata, l'applicazione richiesta viene avviata, arrestata o riavviata nel dispositivo client.

Se si riavvia Network Agent, viene visualizzato un messaggio che indica che la connessione corrente del dispositivo ad Administration Server andrà persa.

Esecuzione della diagnostica remota di Kaspersky Security Center Linux Network Agent e download dei risultati

Per avviare la diagnostica per Kaspersky Security Center Linux Network Agent in un dispositivo remoto e scaricare i risultati:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni, selezionare **Kaspersky Security Center Linux Network Agent**.

   Si apre l'elenco delle opzioni di diagnostica remota.
4. Nella sezione **Rapporto di diagnostica**, fare clic sul pulsante **Esegui diagnostica**.

   In questo modo si avvia la procedura di diagnostica remota e si genera un rapporto di diagnostica. Al termine della procedura di diagnostica, il pulsante **Scarica il rapporto di diagnostica** diventa disponibile.
5. Fare clic sul pulsante **Scarica il rapporto di diagnostica** per scaricare il rapporto.

Il rapporto viene scaricato nella posizione specificata.

Esecuzione di un'applicazione in un dispositivo client

Potrebbe essere necessario eseguire un'applicazione nel dispositivo client, se richiesto da uno specialista dell'assistenza Kaspersky. Non è necessario installare l'applicazione nel dispositivo.

Per eseguire un'applicazione nel dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Esecuzione di un'applicazione remota**.
3. Nella sezione **File dell'applicazione**, fare clic sul pulsante **Sfoglia** per selezionare un archivio ZIP contenente l'applicazione che si desidera eseguire nel dispositivo client.

   L'archivio ZIP deve includere la cartella dell'utilità. Questa cartella contiene il file eseguibile da eseguire in un dispositivo remoto.

È possibile specificare il nome del file eseguibile e gli argomenti della riga di comando, se necessario. A tale scopo, compilare i campi **Executable file in an archive to be run on a remote device** e **Argomenti della riga di comando**.

4. Facendo clic sul pulsante **Carica ed esegui** per eseguire l'applicazione specificata in un dispositivo client.

5. Seguire le istruzioni dell'esperto dell'Assistenza Kaspersky.

Generazione di un file di dump per un'applicazione

Un file di dump dell'applicazione consente di visualizzare i parametri dell'applicazione in esecuzione in un dispositivo client in un determinato momento. Questo file contiene anche informazioni sui moduli che sono stati caricati per un'applicazione.

L'ottenimento dei file di dump da dispositivi basati su Linux non è supportato.

Per ottenere i file di dump tramite la diagnostica remota, viene utilizzata l'utilità kldumper. Questa utilità è progettata per ottenere i file di dump dei processi delle applicazioni Kaspersky su richiesta degli specialisti dell'Assistenza tecnica. Informazioni dettagliate sui requisiti per l'utilizzo dell'utilità kldumper sono fornite nella Knowledge Base di Kaspersky Security Center Linux.

Per creare un file di dump per un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.

2. Nella finestra della diagnostica remota, selezionare la scheda **Esecuzione di un'applicazione remota**.

3. Nella sezione **Generazione del file di dump della memoria del processo in corso**, specificare il file eseguibile dell'applicazione per la quale si desidera generare un file dump.

4. Fare clic sul pulsante **Scarica file di dump**.

   Viene scaricato un archivio con il file di dump per l'applicazione specificata.

   Se l'applicazione specificata non è in esecuzione nel dispositivo client, la cartella "result" contenuta nell'archivio scaricato sarà vuota.

   Se l'applicazione specificata è in esecuzione, ma il download non riesce con un errore o la cartella "result" contenuta nell'archivio scaricato è vuota, fare riferimento alla Knowledge Base di Kaspersky Security Center Linux.

Esecuzione della diagnostica remota in un dispositivo client basato su Linux

Kaspersky Security Center Linux consente di scaricare le informazioni diagnostiche di base da un dispositivo client. In alternativa, è possibile ottenere le informazioni diagnostiche su un dispositivo basato su Linux utilizzando lo script collect.sh di Kaspersky. Questo script viene eseguito nel dispositivo client basato su Linux che deve essere diagnosticato, quindi genera un file con le informazioni diagnostiche, le informazioni di sistema su questo dispositivo, i file di traccia delle applicazioni, i registri del dispositivo e un file di dump per le applicazioni terminate di emergenza.

È consigliabile utilizzare lo script collect.sh per ottenere tutte le informazioni diagnostiche sul dispositivo client basato su Linux contemporaneamente. Se si scaricano le informazioni diagnostiche da remoto tramite Kaspersky Security Center Linux, sarà necessario esaminare tutte le sezioni dell'interfaccia di diagnostica remota. Inoltre, è probabile che le informazioni diagnostiche di un dispositivo basato su Linux non vengano ottenute completamente.

Se è necessario inviare il file generato con le informazioni diagnostiche all'Assistenza tecnica di Kaspersky, eliminare tutte le informazioni riservate prima di inviare il file.

Per scaricare le informazioni diagnostiche da un dispositivo client basato su Linux utilizzando lo script collect.sh:

1. Scaricare lo script collect.sh contenuto nell'archivio collect.tar.gz.
2. Copiare l'archivio scaricato nel dispositivo client basato su Linux da diagnosticare.
3. Eseguire il seguente comando per decomprimere l'archivio collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Eseguire il seguente comando per specificare i diritti di esecuzione dello script:

   ```
   # chmod +x collect.sh
   ```

5. Eseguire lo script collect.sh utilizzando un account con diritti di amministratore:

   ```
   # ./collect.sh
   ```

Un file con le informazioni diagnostiche viene generato e salvato nella cartella /tmp/$HOST_NAME-collect.tar.gz.

Gestione delle applicazioni e dei file eseguibili di terzi nei dispositivi client

Questa sezione descrive le funzionalità di Kaspersky Security Center Linux relative alla gestione delle applicazioni e dei file eseguibili di terzi eseguiti nei dispositivi client.

Utilizzo di Controllo Applicazioni per gestire i file eseguibili

È possibile utilizzare il componente Controllo Applicazioni per consentire o bloccare l'avvio dei file eseguibili nei dispositivi dell'utente. Il componente Controllo Applicazioni supporta i sistemi operativi basati su Windows e Linux.

Per i sistemi operativi basati su Linux, il componente Controllo Applicazioni è disponibile a partire da Kaspersky Endpoint Security 11.2 for Linux.

Prerequisiti

- Kaspersky Security Center Linux viene distribuito nell'organizzazione.
- Il criterio di Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security for Windows è stato creato ed è attivo. Il componente Controllo Applicazioni è abilitato nel criterio.

Passaggi

Lo scenario di utilizzo di Controllo Applicazioni prevede diversi passaggi:

1. **Creazione e visualizzazione dell'elenco dei file eseguibili nei dispositivi client**

   Questo passaggio consente di scoprire quali file eseguibili sono presenti nei dispositivi gestiti. Visualizzare l'elenco dei file eseguibili e confrontarlo con l'elenco dei file eseguibili consentiti e non consentiti. Le restrizioni relative all'utilizzo dei file eseguibili possono essere correlate ai criteri di sicurezza delle informazioni dell'organizzazione.

   Istruzioni dettagliate: Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client

2. **Creazione di categorie per i file eseguibili utilizzati nell'organizzazione**

   Analizzare gli elenchi dei file eseguibili archiviati nei dispositivi gestiti. In base all'analisi, creare categorie per i file eseguibili. È consigliabile creare una categoria "Applicazioni di lavoro" che includa il set standard di file eseguibili utilizzati nell'organizzazione. Se differenti gruppi di sicurezza utilizzano i propri set di file eseguibili nel proprio lavoro, è possibile creare una categoria distinta per ciascun gruppo di sicurezza.

   L'avvio di file eseguibili le cui impostazioni non corrispondono ad alcuna delle regole di Controllo Applicazioni è regolato dalla modalità operativa selezionata del componente:

   - *Lista vietati.* La modalità viene utilizzata se si desidera consentire l'avvio di tutti i file eseguibili tranne quelli specificati nelle regole di blocco. Questa modalità è selezionata per impostazione predefinita.
   - *Lista consentiti.* La modalità viene utilizzata se si desidera bloccare l'avvio di tutti i file eseguibili tranne quelli specificati nelle regole di permesso.

   Le regole di Controllo Applicazioni sono implementate tramite categorie per i file eseguibili. In Kaspersky Security Center Linux, esistono tre tipi di categorie di file eseguibili:

- Categoria con contenuto aggiunto manualmente. Vengono definite le condizioni (ad esempio, metadati del file, codice hash del file, certificato del file o percorso del file) per includere i file eseguibili nella categoria.
- Categoria che include i file eseguibili dei dispositivi selezionati. Viene specificato un dispositivo che contiene i file eseguibili inclusi automaticamente nella categoria.
- Categoria che include i file eseguibili in una cartella selezionata. Viene specificata una cartella che contiene i file eseguibili inclusi automaticamente nella categoria.

3. **Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security**

   Configurare il componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Linux utilizzando le categorie create nel passaggio precedente.

   Istruzioni dettagliate: Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows

4. **Attivazione del componente Controllo Applicazioni in modalità di test**

   Per garantire che le regole di Controllo Applicazioni non blocchino i file eseguibili richiesti per il lavoro dell'utente, è consigliabile abilitare il test delle regole di Controllo Applicazioni e analizzarne il funzionamento dopo aver creato le nuove regole. Quando il test è abilitato, Kaspersky Endpoint Security for Windows non bloccherà i file eseguibili il cui avvio non è consentito dalle regole di Controllo Applicazioni, ma invierà invece notifiche sul relativo avvio ad Administration Server.

   Durante il test delle regole di Controllo Applicazioni, è consigliabile eseguire le seguenti azioni:

   - Determinare il periodo di test. Il periodo di test può variare da alcuni giorni a due mesi.
   - Esaminare gli eventi risultanti dal test del funzionamento di Controllo Applicazioni.

   Istruzioni dettagliate per Kaspersky Security Center Web Console: Configurazione del componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows. Seguire queste istruzioni e abilitare l'opzione **Modalità test** nel processo di configurazione.

5. **Modifica delle impostazioni del componente Controllo Applicazioni**

   Se necessario, apportare modifiche alle impostazioni di Controllo Applicazioni. In base ai risultati del test, è possibile aggiungere i file eseguibili correlati agli eventi del componente Controllo Applicazioni a una categoria con contenuto aggiunto manualmente.

   Istruzioni dettagliate: Kaspersky Security Center Web Console: Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni

6. **Applicazione delle regole di Controllo Applicazioni in modalità operativa**

   Dopo aver testato le regole di Controllo Applicazioni e completato la configurazione delle categorie, è possibile applicare le regole di Controllo Applicazioni in modalità operativa.

   Istruzioni dettagliate per Kaspersky Security Center Web Console: Configurazione del componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows. Seguire queste istruzioni e disabilitare l'opzione **Modalità test** nel processo di configurazione.

7. **Verifica della configurazione di Controllo Applicazioni**

   Assicurarsi di avere eseguito le seguenti operazioni:

   - Categorie create per i file eseguibili.
   - Configurazione di Controllo Applicazioni tramite le categorie.
   - Applicazione delle regole di Controllo Applicazioni in modalità operativa.

Risultati

Al termine dello scenario, viene controllato l'avvio dei file eseguibili nei dispositivi gestiti. Gli utenti possono eseguire solo i file eseguibili consentiti nell'organizzazione e non possono eseguire quelli non consentiti.

Per informazioni dettagliate su Controllo Applicazioni, consultare la Guida di Kaspersky Endpoint Security for Linux e la Guida di Kaspersky Endpoint Security for Windows.

Modalità e categorie di Controllo Applicazioni

Il componente Controllo Applicazioni monitora i tentativi degli utenti di avviare i file eseguibili. È possibile utilizzare le regole di Controllo Applicazioni per controllare l'avvio dei file eseguibili.

Il componente Controllo Applicazioni è disponibile per Kaspersky Endpoint Security 11.2 for Linux e versioni successive.

L'avvio di file eseguibili le cui impostazioni non corrispondono ad alcuna delle regole di Controllo Applicazioni è regolato dalla modalità operativa selezionata del componente:

- *Lista vietati*. La modalità viene utilizzata se si desidera consentire l'avvio di tutti i file eseguibili tranne quelli specificati nelle regole di blocco. Questa modalità è selezionata per impostazione predefinita.
- *Lista consentiti*. La modalità viene utilizzata se si desidera bloccare l'avvio di tutti i file eseguibili tranne quelli specificati nelle regole di permesso.

Le regole di Controllo Applicazioni sono implementate tramite categorie per i file eseguibili. In Kaspersky Security Center Linux, esistono tre tipi di categorie:

- Categoria con contenuto aggiunto manualmente. Vengono definite le condizioni (ad esempio, metadati del file, codice hash del file, certificato del file o percorso del file) per includere i file eseguibili nella categoria.
- Categoria che include i file eseguibili dei dispositivi selezionati. Viene specificato un dispositivo che contiene i file eseguibili inclusi automaticamente nella categoria.
- Categoria che include i file eseguibili in una cartella selezionata. Viene specificata una cartella che contiene i file eseguibili inclusi automaticamente nella categoria.

Per informazioni dettagliate su Controllo Applicazioni, consultare la Guida di Kaspersky Endpoint Security for Linux e la Guida di Kaspersky Endpoint Security for Windows.

Recupero e visualizzazione di un elenco delle applicazioni installate nei dispositivi client

Kaspersky Security Center Linux esegue l'inventario di tutto il software installato nei dispositivi client gestiti che eseguono Linux e Windows.

Network Agent compila un elenco delle applicazioni installate in un dispositivo, quindi trasmette questo elenco ad Administration Server. Sono necessari circa 10-15 minuti affinché Network Agent aggiorni l'elenco delle applicazioni.

Per i dispositivi client basati su Windows, Network Agent riceve la maggior parte delle informazioni sulle applicazioni installate dal Registro di sistema di Windows. Per i dispositivi client basati su Linux, gli strumenti di gestione di pacchetti forniscono informazioni sulle applicazioni installate a Network Agent.

Per visualizzare l'elenco delle applicazioni installate nei dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Registro delle applicazioni**.

   Nella pagina viene visualizzata una tabella con le applicazioni installate nei dispositivi gestiti. Selezionare l'applicazione per visualizzarne le proprietà, ad esempio il nome del fornitore, il numero di versione, l'elenco dei file eseguibili, l'elenco dei dispositivi in cui è installata l'applicazione.

2. È possibile raggruppare e filtrare i dati della tabella con le applicazioni installate come segue:

   - Fare clic sull'icona delle impostazioni ( ) nell'angolo superiore destro della tabella.

     Nel menu **Impostazioni colonne** richiamato, selezionare le colonne da visualizzare nella tabella. Per visualizzare il tipo di sistema operativo dei dispositivi client in cui è installata l'applicazione, selezionare la colonna **Tipo di sistema operativo**.

   - Fare clic sull'icona del filtro ( ) nell'angolo superiore destro della tabella, quindi specificare e applicare il criterio di filtro nel menu richiamato.

     Viene visualizzata la tabella filtrata delle applicazioni installate.

Per visualizzare l'elenco delle applicazioni installate in un dispositivo gestito specifico:

Nel menu principale accedere a **Dispositivi** → **Dispositivi gestiti** → **<nome dispositivo>** → **Avanzate** → **Registro delle applicazioni**. In questo menu, è possibile esportare l'elenco delle applicazioni in un file CSV o TXT.

Per informazioni dettagliate su Controllo Applicazioni, consultare la Guida di Kaspersky Endpoint Security for Linux e la Guida di Kaspersky Endpoint Security for Windows.

Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client

È possibile ottenere l'elenco dei file eseguibili archiviati sui dispositivi client in uno dei seguenti modi:

- Abilitazione delle notifiche sull'avvio delle applicazioni nel criterio di Kaspersky Endpoint Security.
- Creazione di un'attività di inventario.

Abilitazione delle notifiche sull'avvio delle applicazioni nel criterio di Kaspersky Endpoint Security

Per abilitare le notifiche sull'avvio delle applicazioni:

1. Aprire le impostazioni dei criteri di Kaspersky Endpoint Security, quindi passare a **Impostazioni generali** → **Rapporti e archivi**.
2. Nel gruppo di impostazioni **Trasferimento dati ad Administration Server**, selezionare la casella di controllo **Informazioni sulle applicazioni avviate** e salvare le modifiche.

Quando un utente tenta di avviare file eseguibili, le informazioni su tali file vengono aggiunte all'elenco dei file eseguibili su un dispositivo client. Kaspersky Endpoint Security invia queste informazioni a Network Agent, che a sua volta le invia ad Administration Server.

Creazione di un'attività di inventario

Per Kaspersky Endpoint Security for Linux, la funzionalità di inventario dei file eseguibili è disponibile solo a partire della versione 11.2.

È possibile ridurre il carico sul database mentre si ottengono informazioni sulle applicazioni installate. Per risparmiare spazio nel database, eseguire un'attività di inventario sui dispositivi di riferimento in cui è installato un set standard di software. Il numero preferibile di dispositivi è 1-3.

Per creare un'attività di inventario per i file eseguibili nei dispositivi client:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

   Verrà visualizzato l'elenco delle attività.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

3. Nella pagina **Nuova attività**, nell'elenco a discesa **Applicazione**, selezionare Kaspersky Endpoint Security for Linux o Kaspersky Endpoint Security for Windows, a seconda del sistema operativo dei dispositivi client.

4. Nell'elenco a discesa **Tipo di attività** selezionare **Inventario**.

5. Nella pagina **Completa creazione attività** fare clic sul pulsante **Fine**.

   Al termine della Creazione guidata nuova attività, l'attività **Inventario** sarà creata e configurata. Se si desidera, è possibile modificare le impostazioni per l'attività creata. La nuova attività creata verrà visualizzata nell'elenco delle attività.

Per una descrizione dettagliata dell'attività di inventario, consultare la Guida di Kaspersky Endpoint Security for Linux e la Guida di Kaspersky Endpoint Security for Windows.

Dopo l'esecuzione dell'attività **Inventario**, viene formato l'elenco dei file eseguibili archiviati nei dispositivi gestiti ed è possibile visualizzarlo.

Durante l'esecuzione dell'attività di inventario, è possibile rilevare file eseguibili nei seguenti formati (a seconda dell'opzione selezionata nelle proprietà dell'attività di inventario): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Visualizzazione dell'elenco dei file eseguibili archiviati nei dispositivi gestiti

Per visualizzare l'elenco dei file eseguibili archiviati nei dispositivi client:

Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **File eseguibili**.

La pagina visualizzerà l'elenco dei file eseguibili archiviati nei dispositivi client.

Se necessario, è possibile inviare il file eseguibile del dispositivo gestito al dispositivo su cui è aperta Kaspersky Security Center Web Console.

Per inviare un file eseguibile:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → File eseguibili**.
2. Fare clic sul collegamento del file eseguibile che si desidera inviare.
3. Nella finestra visualizzata, accedere alla sezione **Dispositivi**, quindi selezionare la casella di controllo del dispositivo gestito da cui si desidera inviare il file eseguibile.

   Prima di inviare il file eseguibile, assicurarsi che il dispositivo gestito disponga di una connessione diretta ad Administration Server selezionando la casella di controllo **Non eseguire la disconnessione da Administration Server**.

4. Fare clic sul pulsante **Invia**.

Il file eseguibile selezionato viene scaricato per essere inviato al dispositivo su cui è aperta Kaspersky Security Center Web Console.

Creazione di una categoria di applicazioni con contenuto aggiunto manualmente

È possibile specificare un set di criteri come modello per i file eseguibili di cui consentire o bloccare l'avvio nell'organizzazione. In base ai file eseguibili corrispondenti ai criteri, è possibile creare una categoria di applicazioni e utilizzarla nella configurazione del componente Controllo Applicazioni.

Per creare una categoria di applicazioni con contenuto aggiunto manualmente:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Categorie di applicazioni**.

   Verrà visualizzata la pagina con un elenco di categorie di applicazioni.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova categoria. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nel passaggio **Selezionare il metodo di creazione della categoria**, specificare il nome della categoria di applicazioni e selezionare l'opzione **Categoria con contenuto aggiunto manualmente. I dati dei file eseguibili vengono aggiunti alla categoria in modo manuale**.

4. Nel passaggio **Condizioni** fare clic sul pulsante **Aggiungi** per aggiungere un criterio di condizione per includere i file nella creazione della categoria.

5. Nel passaggio **Criteri condizione** selezionare un tipo di regola per la creazione della categoria dall'elenco:

   - Da categoria KL

Se questa opzione è selezionata, è possibile specificare una categoria di applicazioni Kaspersky come condizione per l'aggiunta di applicazioni alla categoria utente. Le applicazioni della categoria Kaspersky specificata verranno aggiunte alla categoria utente di applicazioni.

- Seleziona certificato dall'archivio

  Se questa opzione è selezionata, è possibile specificare i certificati dell'archivio. La condizione di categoria corrisponde solo ai file eseguibili firmati dal certificato specificato.

- Specificare il percorso dell'applicazione (maschere supportate)

  Se questa opzione è selezionata, è possibile specificare il percorso di una cartella nel dispositivo client che contiene i file eseguibili da aggiungere alla categoria utente di applicazioni.

- Unità rimovibile

  Se questa opzione è selezionata, è possibile specificare il tipo di supporto (qualsiasi unità o unità rimovibile) in cui viene eseguita l'applicazione. Le applicazioni che sono state eseguite nel tipo di unità selezionato verranno aggiunte alla categoria utente di applicazioni.

- **Hash, metadati o certificato**:

  - Selezionare dall'elenco dei file eseguibili

    Se questa opzione è selezionata, è possibile utilizzare l'elenco dei file eseguibili nel dispositivo client per selezionare e aggiungere applicazioni alla categoria.

  - Selezionare dal registro delle applicazioni

    Se questa opzione è selezionata, viene visualizzato il registro delle applicazioni. Dopo aver selezionato un'applicazione dal registro, viene aperta una finestra con i parametri compilati con i metadati dell'applicazione selezionata:

    - Nome file.
    - Versione file. È possibile specificare un valore preciso per la versione o descrivere una condizione, ad esempio "maggiore di 5.0".
    - Nome applicazione.
    - Versione applicazione. È possibile specificare un valore preciso per la versione o descrivere una condizione, ad esempio "maggiore di 5.0".
    - Vendor.

    Viene bloccato solo l'avvio dei file eseguibili che soddisfano i parametri specificati, non l'avvio dell'applicazione selezionata. Se i metadati dell'applicazione selezionata corrispondono a quelli del file eseguibile avviato all'avvio dell'applicazione, è possibile procedere al passaggio successivo. In caso contrario, è necessario modificare manualmente i valori in modo che corrispondano ai metadati del file eseguibile.

- Specificare manualmente

  Se questa opzione è selezionata, è necessario specificare l'hash del file, i metadati o un certificato come condizione per l'aggiunta di applicazioni alla categoria utente.

  Hash del file

  A seconda della versione dell'applicazione di protezione installata nei dispositivi della rete, è necessario selezionare un algoritmo per il calcolo del valore hash da parte di Kaspersky Security Center Linux per i file di questa categoria. Le informazioni sui valori hash calcolati dalle funzioni hash vengono memorizzate nel database di Administration Server.

  SHA256 è una funzione hash di criptaggio: non sono state rilevate vulnerabilità nell'algoritmo, pertanto è considerata la più affidabile funzione di criptaggio attualmente disponibile. Kaspersky Endpoint Security for Linux supporta il calcolo SHA256.

  Selezionare una delle opzioni di calcolo del valore hash da parte di Kaspersky Security Center Linux per i file della categoria:

  - Se tutte le istanze delle applicazioni di protezione installate nella rete sono Kaspersky Endpoint Security for Linux, selezionare la casella di controllo **SHA-256**.
  - Selezionare la casella di controllo **Hash MD5** solo se si utilizza Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux non supporta la funzione hash MD5.

  Metadati

  Se questa opzione è selezionata, è possibile specificare i metadati del file, come il nome del file, la versione del file o il fornitore. La condizione di categoria corrisponde solo ai file eseguibili con gli stessi metadati.

  Certificato

  Se questa opzione è selezionata, è possibile specificare i certificati dell'archivio. La condizione di categoria corrisponde solo ai file eseguibili firmati dal certificato specificato.

- Dalla cartella archiviata

  Se questa opzione è selezionata, è possibile specificare un file di una cartella archiviata, quindi selezionare la condizione che si desidera utilizzare per aggiungere applicazioni alla categoria utente. La cartella archiviata viene decompressa e le condizioni selezionate vengono applicate ai file nella cartella. Come condizione è possibile selezionare uno dei seguenti criteri:

  - **Hash del file**

    Selezionare la funzione hash (MD5 o SHA256) che si desidera utilizzare per calcolare i valori hash. Le applicazioni con lo stesso valore hash dei file nella cartella archiviata verranno aggiunte alla categoria di applicazioni dell'utente.

    Selezionare una funzione hash MD5 solo se si utilizza Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux non supporta la funzione hash MD5.

  - **Metadati**

    Selezionare i metadati che si desidera utilizzare come criteri. I file eseguibili che contengono gli stessi metadati verranno aggiunti alla categoria utente di applicazioni.

  - **Certificato**

    Selezionare le proprietà del certificato (oggetto del certificato, impronta digitale o emittente) che si desidera utilizzare come criteri. I file eseguibili firmati con i certificati che dispongono delle stesse proprietà verranno aggiunti alla categoria utente.

Se questa opzione è selezionata, è possibile specificare un file di una cartella archiviata, quindi selezionare la condizione che si desidera utilizzare per aggiungere applicazioni alla categoria utente. La cartella archiviata viene decompressa e le condizioni selezionate vengono applicate ai file nella cartella. Come condizione è possibile selezionare uno dei seguenti criteri:

- **Hash del file**

  Selezionare la funzione hash (MD5 o SHA256) che si desidera utilizzare per calcolare i valori hash. Le applicazioni con lo stesso valore hash dei file nella cartella archiviata verranno aggiunte alla categoria di applicazioni dell'utente.

  Selezionare una funzione hash MD5 solo se si utilizza Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux non supporta la funzione hash MD5.

- **Metadati**

  Selezionare i metadati che si desidera utilizzare come criteri. I file eseguibili che contengono gli stessi metadati verranno aggiunti alla categoria utente di applicazioni.

- **Certificato**

  Selezionare le proprietà del certificato (oggetto del certificato, impronta digitale o emittente) che si desidera utilizzare come criteri. I file eseguibili firmati con i certificati che dispongono delle stesse proprietà verranno aggiunti alla categoria utente.

Il criterio selezionato viene aggiunto all'elenco delle condizioni.

È possibile aggiungere tutti i criteri necessari per la creazione della categoria di applicazioni.

6. Nel passaggio **Esclusioni** fare clic sul pulsante **Aggiungi** per aggiungere un criterio di condizione esclusivo per escludere i file dalla categoria creata.

7. Nel passaggio **Criteri condizione** selezionare un tipo di regola dall'elenco, nello stesso modo in cui è stato selezionato un tipo di regola per la creazione della categoria.

Al termine della procedura guidata, viene creata la categoria di applicazioni. La regola è visualizzata nell'elenco delle categorie di applicazioni. È possibile utilizzare la categoria di applicazioni creata durante la configurazione di Controllo Applicazioni.

Per informazioni dettagliate su Controllo Applicazioni, consultare la Guida di Kaspersky Endpoint Security for Linux e la Guida di Kaspersky Endpoint Security for Windows.

Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati

È possibile utilizzare i file eseguibili nei dispositivi selezionati come modello per i file eseguibili da consentire o bloccare. In base ai file eseguibili nei dispositivi selezionati, è possibile creare una categoria di applicazioni e utilizzarla nella configurazione del componente Controllo Applicazioni.

Assicurarsi che vengano soddisfatti i seguenti prerequisiti:

- Il componente Controllo Applicazioni è abilitato nel criterio di Kaspersky Endpoint Security.
- È stato ottenuto un elenco di file eseguibili archiviati nei dispositivi gestiti.

Per creare una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Categorie di applicazioni**.

   Viene visualizzata la pagina con un elenco di categorie di file eseguibili.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova categoria. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nel passaggio **Selezionare il metodo di creazione della categoria**, specificare il nome della categoria e selezionare l'opzione **Categoria che include i file eseguibili dei dispositivi selezionati. Tali file eseguibili sono elaborati automaticamente e le relative metriche vengono aggiunte alla categoria**.

4. Fare clic su **Aggiungi**.

5. Nella finestra visualizzata selezionare uno o più dispositivi che contengono i file eseguibili da utilizzare per creare la categoria di applicazioni.

6. Specificare le seguenti impostazioni:

   - Algoritmo di calcolo del valore hash

     A seconda della versione dell'applicazione di protezione installata nei dispositivi della rete, è necessario selezionare un algoritmo per il calcolo del valore hash da parte di Kaspersky Security Center Linux per i file di questa categoria. Le informazioni sui valori hash calcolati dalle funzioni hash vengono memorizzate nel database di Administration Server.

     SHA256 è una funzione hash di criptaggio: non sono state rilevate vulnerabilità nell'algoritmo, pertanto è considerata la più affidabile funzione di criptaggio attualmente disponibile. Kaspersky Endpoint Security for Linux supporta il calcolo SHA256.

     Selezionare una delle opzioni di calcolo del valore hash da parte di Kaspersky Security Center Linux per i file della categoria:

     - Se tutte le istanze delle applicazioni di protezione installate nella rete sono Kaspersky Endpoint Security for Linux, selezionare la casella di controllo **SHA-256**.

     Selezionare la casella di controllo **Hash MD5** solo se si utilizza Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux non supporta la funzione hash MD5.

     La casella di controllo **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)** è selezionata per impostazione predefinita.

     La casella di controllo **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** è deselezionata per impostazione predefinita.

   - Sincronizza i dati con l'archivio dell'Administration Server

     Selezionare questa opzione se si desidera che Administration Server controlli periodicamente le modifiche nelle cartelle specificate.

     Per impostazione predefinita, questa opzione è disabilitata.

     Se si abilita questa opzione, specificare il periodo (in ore) per la verifica delle modifiche nelle cartelle specificate. Per impostazione predefinita, l'intervallo per la scansione è di 24 ore.

   - Tipo di file

In questa sezione è possibile specificare il tipo di file utilizzato per creare la categoria di applicazioni.

Tutti i file. Durante la creazione della categoria vengono presi in considerazione tutti i file. Per impostazione predefinita, questa opzione è selezionata.

Solo i file esterni alle categorie di applicazioni. Durante la creazione della categoria vengono presi in considerazione solo i file esterni alle categorie di applicazioni.

- Cartelle

  In questa sezione è possibile specificare quali cartelle nei dispositivi selezionati contengono i file utilizzati per creare la categoria di applicazioni.

  Tutte le cartelle. Per la creazione della categoria vengono prese in considerazione tutte le cartelle. Per impostazione predefinita, questa opzione è selezionata.

  Cartella specificata. Per la creazione della categoria viene presa in considerazione solo la cartella specificata. Se si seleziona questa opzione, è necessario specificare il percorso della cartella.

Al termine della procedura guidata, viene creata la categoria di file eseguibili. La regola è visualizzata nell'elenco delle categorie. È possibile utilizzare la categoria creata durante la configurazione di Controllo Applicazioni.

Creazione di una categoria di applicazioni che include i file eseguibili in una cartella selezionata

È possibile utilizzare i file eseguibili in una cartella selezionata come standard per i file eseguibili da consentire o bloccare nell'organizzazione. In base ai file eseguibili nella cartella selezionata, è possibile creare una categoria di applicazioni e utilizzarla nella configurazione del componente Controllo Applicazioni.

Per creare una categoria che include i file eseguibili in una cartella selezionata:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Categorie di applicazioni**.

   Verrà visualizzata la pagina con un elenco di categorie.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova categoria. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nel passaggio **Selezionare il metodo di creazione della categoria** specificare il nome della categoria e selezionare l'opzione **Categoria che include file eseguibili di una cartella specifica. I file eseguibili delle applicazioni copiati nella cartella specificata sono elaborati automaticamente e le relative metriche vengono aggiunte alla categoria**.

4. Specificare la cartella i cui file eseguibili verranno utilizzati per creare la categoria.

5. Definire le seguenti impostazioni:

   - Includi librerie di collegamento dinamico (DLL) in questa categoria

La categoria di applicazioni include le librerie di collegamento dinamico (file in formato DLL) e il componente Controllo Applicazioni registra le azioni di tali librerie in esecuzione nel sistema. L'inclusione dei file DLL nella categoria può ridurre le prestazioni di Kaspersky Security Center.

Per impostazione predefinita, questa casella di controllo è deselezionata.

- Includi i dati degli script in questa categoria

  La categoria di applicazioni include i dati sugli script e gli script non vengono bloccati da Protezione minacce Web. L'inclusione dei dati sugli script nella categoria può ridurre le prestazioni di Kaspersky Security Center.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Algoritmo di calcolo del valore hash: **Calcola SHA-256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)** / **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

  A seconda della versione dell'applicazione di protezione installata nei dispositivi della rete, è necessario selezionare un algoritmo per il calcolo del valore hash da parte di Kaspersky Security Center Linux per i file di questa categoria. Le informazioni sui valori hash calcolati dalle funzioni hash vengono memorizzate nel database di Administration Server.

  SHA256 è una funzione hash di criptaggio: non sono state rilevate vulnerabilità nell'algoritmo, pertanto è considerata la più affidabile funzione di criptaggio attualmente disponibile. Kaspersky Endpoint Security for Linux supporta il calcolo SHA256.

  Selezionare una delle opzioni di calcolo del valore hash da parte di Kaspersky Security Center Linux per i file della categoria:

  - Se tutte le istanze delle applicazioni di protezione installate nella rete sono Kaspersky Endpoint Security for Linux, selezionare la casella di controllo **SHA-256**.

  Selezionare la casella di controllo **Hash MD5** solo se si utilizza Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux non supporta la funzione hash MD5.

  La casella di controllo **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)** è selezionata per impostazione predefinita.

  La casella di controllo **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** è deselezionata per impostazione predefinita.

- Forza scansione delle modifiche nella cartella

  Se questa opzione è abilitata, l'applicazione controlla periodicamente la presenza di modifiche nella cartella di aggiunta di contenuto nelle categorie. È possibile specificare la frequenza dei controlli (in ore) nel campo di immissione accanto alla casella di controllo. Per impostazione predefinita, l'intervallo di tempo fra i controlli forzati è di 24 ore.

  Se questa opzione è disabilitata, non verranno forzati controlli della cartella. Il server tenta di accedere ai file modificati, aggiunti o eliminati.

  Per impostazione predefinita, questa opzione è disabilitata.

Al termine della procedura guidata, viene creata la categoria di file eseguibili. La regola è visualizzata nell'elenco delle categorie. È possibile utilizzare la categoria nella configurazione di Controllo Applicazioni.

Per informazioni dettagliate su Controllo Applicazioni, consultare la Guida di Kaspersky Endpoint Security for Linux e la Guida di Kaspersky Endpoint Security for Windows.

Visualizzazione dell'elenco delle categorie di applicazioni

È possibile visualizzare l'elenco delle categorie di file eseguibili configurate e le impostazioni di ciascuna categoria.

Per visualizzare l'elenco delle categorie di applicazioni:

Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Categorie di applicazioni**.

Verrà visualizzata la pagina con un elenco di categorie.

Per visualizzare le proprietà di una categoria di applicazioni:

Fare clic sul nome della categoria.

Verrà visualizzata la finestra delle proprietà della categoria. Le proprietà sono raggruppate in diverse schede.

Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows

Dopo aver creato le categorie di Controllo Applicazioni, è possibile utilizzarle per configurare Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows.

Per configurare Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

   Verrà visualizzata una pagina con un elenco di criteri.

2. Fare clic sul criterio **Kaspersky Endpoint Security for Windows**.

   Verrà visualizzata la finestra delle impostazioni del criterio.

3. Passare a **Impostazioni applicazione** → **Security Controls** → **Application Control**.

   Verrà visualizzata la finestra **Controllo Applicazioni** con le impostazioni di Controllo Applicazioni.

4. L'opzione **Controllo Applicazioni** è abilitata per impostazione predefinita. Spostare l'interruttore su **Controllo Applicazioni DISABILITATO** per disabilitare l'opzione.

5. Nelle impostazioni del blocco **Impostazioni di Controllo Applicazioni**, abilitare la modalità operativa per applicare le regole di Controllo applicazioni e consentire a Kaspersky Endpoint Security for Windows di bloccare l'avvio delle applicazioni.

   Se si desidera testare le regole di Controllo Applicazioni, nella sezione **Impostazioni di Controllo Applicazioni**, abilitare la modalità di test. In modalità di test, Kaspersky Endpoint Security for Windows non blocca l'avvio delle applicazioni, ma registra le informazioni sulle regole attivate nel rapporto. Fare clic sul collegamento **Visualizza rapporto** per visualizzare queste informazioni.

6. Abilitare l'opzione **Controlla il caricamento dei moduli DLL** se si desidera che Kaspersky Endpoint Security for Windows monitori il caricamento dei moduli DLL all'avvio delle applicazioni da parte degli utenti.

   Le informazioni sul modulo e sull'applicazione che ha caricato il modulo verranno salvate in un rapporto.

   Kaspersky Endpoint Security for Windows monitora solo i moduli DLL e i driver caricati dopo che è stata selezionata l'opzione **Controlla il caricamento dei moduli DLL**. Riavviare il dispositivo dopo aver selezionato l'opzione **Controlla il caricamento dei moduli DLL** se si desidera che Kaspersky Endpoint Security for Windows monitori tutti i moduli DLL e i driver, inclusi quelli caricati prima dell'avvio di Kaspersky Endpoint Security for Windows.

7. (Facoltativo) Nella sezione **Modelli di messaggi** modificare il modello del messaggio visualizzato quando l'avvio di un'applicazione è bloccato e il modello del messaggio e-mail inviato.

8. Nelle impostazioni del gruppo **Modalità Controllo Applicazioni**, selezionare la modalità **Lista vietati** o **Lista consentiti**.

   Per impostazione predefinita, è selezionata la modalità **Lista vietati**.

9. Fare clic sul collegamento **Impostazioni elenchi di regole**.

   Verrà visualizzata la finestra **Liste vietati e Liste consentiti** per consentire di aggiungere una categoria di applicazioni. Per impostazione predefinita, è selezionata la scheda **Lista vietati** se è selezionata la modalità **Lista vietati** e la scheda **Lista consentiti** se è selezionata la modalità **Lista consentiti**.

10. Nella finestra **Liste vietati e liste consentiti** fare clic sul pulsante **Aggiungi**.

    Verrà visualizzata la finestra **Regola di Controllo Applicazioni**.

11. Fare clic sul collegamento **Scegliere una categoria**.

    Verrà visualizzata la finestra **Categoria di applicazioni**.

12. Aggiungere una o più categorie di applicazioni create in precedenza.

    È possibile modificare le impostazioni di una categoria creata facendo clic sul pulsante **Modifica**.

    È possibile creare una nuova categoria facendo clic sul pulsante **Aggiungi**.

    È possibile eliminare una categoria dall'elenco facendo clic sul pulsante **Elimina**.

13. Al termine della creazione dell'elenco delle categorie di applicazioni, fare clic sul pulsante **OK**.

    La finestra **Categoria di applicazioni** verrà chiusa.

14. Nella finestra **Regola di Controllo Applicazioni**, nella sezione **Soggetti e relativi diritti**, creare un elenco di utenti e gruppi di utenti a cui applicare la regola di Controllo Applicazioni.

15. Fare clic sul pulsante **OK** per salvare le impostazioni e chiudere la finestra **Regola di Controllo Applicazioni**.

16. Fare clic sul pulsante **OK** per salvare le impostazioni e chiudere la finestra **Liste vietati e liste consentiti**.

17. Fare clic sul pulsante **OK** per salvare le impostazioni e chiudere la finestra **Controllo Applicazioni**.

18. Chiudere la finestra con le impostazioni dei criteri di Kaspersky Endpoint Security for Windows.

Controllo Applicazioni è configurato. Una volta propagato il criterio ai dispositivi client, viene gestito l'avvio dei file eseguibili.

Per informazioni dettagliate su Controllo Applicazioni, consultare la Guida di Kaspersky Endpoint Security for Linux e la Guida di Kaspersky Endpoint Security for Windows.

Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni

Dopo aver configurato Controllo Applicazioni nei criteri di Kaspersky Endpoint Security, i seguenti eventi verranno visualizzati nell'elenco degli eventi:

- **Avvio dell'applicazione non consentito** (evento *Critico*). Questo evento viene visualizzato se è stato configurato Controllo Applicazioni per l'applicazione delle regole.
- **Avvio dell'applicazione non consentito in modalità test** (evento *Informazioni*). Questo evento viene visualizzato se è stato configurato Controllo Applicazioni per il test delle regole.
- **Messaggio all'amministratore sul divieto di avvio dell'applicazione** (evento di *avviso*). Questo evento viene visualizzato se è stato configurato Controllo Applicazioni per l'applicazione delle regole e un utente ha richiesto l'accesso a un'applicazione che è bloccata all'avvio.

È consigliabile creare selezioni eventi per visualizzare gli eventi relativi all'esecuzione di Controllo Applicazioni.

È possibile aggiungere i file eseguibili relativi agli eventi di Controllo Applicazioni a una categoria di applicazioni esistente o a una nuova categoria di applicazioni. È possibile aggiungere i file eseguibili solo a una categoria di applicazioni con contenuto aggiunto manualmente.

Per aggiungere file eseguibili relativi agli eventi di Controllo Applicazioni a una categoria di applicazioni:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.

   Verrà visualizzato l'elenco di selezioni eventi.

2. Selezionare la selezione eventi per visualizzare gli eventi relativi a Controllo Applicazioni e avviare questa selezione eventi.

   Se non è stata creata la selezione eventi correlata a Controllo Applicazioni, è possibile selezionare e avviare una selezione predefinita, ad esempio **Eventi recenti**.

   Verrà visualizzato l'elenco degli eventi.

3. Selezionare gli eventi di cui si desidera aggiungere i file eseguibili associati alla categoria di applicazioni, quindi fare clic sul pulsante **Assegna a categoria**.

   Verrà avviata la Creazione guidata nuova categoria. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Nella pagina della procedura guidata, specificare le impostazioni appropriate:

   - Nella sezione **Azione sul file eseguibile relativo all'evento** selezionare una delle seguenti opzioni:

     - **Aggiungi a una nuova categoria di applicazioni**

       Selezionare questa opzione se si desidera creare una nuova categoria di applicazioni basata sui file eseguibili correlati agli eventi.

       Per impostazione predefinita, questa opzione è selezionata.

       Se è stata selezionata questa opzione, specificare un nuovo nome di categoria.

     - **Aggiungi a una categoria di applicazioni esistente**

Selezionare questa opzione se si desidera aggiungere i file eseguibili correlati agli eventi a una categoria di applicazioni esistente.

Per impostazione predefinita, questa opzione non è selezionata.

Se è stata selezionata questa opzione, selezionare la categoria di applicazioni con contenuto aggiunto manualmente a cui si desidera aggiungere file eseguibili.

- Nella sezione **Tipo di regola** selezionare una delle seguenti opzioni:
  - **Regole per l'aggiunta alle inclusioni**
  - **Regole per l'aggiunta alle esclusioni**
- Nella sezione **Parametro utilizzato come condizione** selezionare una delle seguenti opzioni:
  - Dettagli del certificato (o hash SHA-256 per i file senza certificato)

    I file possono essere firmati con un certificato. Più file possono essere firmati con lo stesso certificato. Ad esempio, lo stesso certificato può essere utilizzato per firmare differenti versioni della stessa applicazione o diverse applicazioni dello stesso fornitore. Quando si seleziona un certificato, possono essere inserite nella categoria diverse versioni di un'applicazione o diverse applicazioni dello stesso fornitore.

    Ogni file dispone di una specifica funzione hash SHA256 univoca. Quando si seleziona una funzione hash SHA256, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

    Selezionare questa opzione se si desidera aggiungere alle regole della categoria i dettagli del certificato di un file eseguibile (o la funzione hash SHA256 per i file senza certificato).

    Per impostazione predefinita, questa opzione è selezionata.

  - Dettagli del certificato (i file senza certificato verranno ignorati)

    I file possono essere firmati con un certificato. Più file possono essere firmati con lo stesso certificato. Ad esempio, lo stesso certificato può essere utilizzato per firmare differenti versioni della stessa applicazione o diverse applicazioni dello stesso fornitore. Quando si seleziona un certificato, possono essere inserite nella categoria diverse versioni di un'applicazione o diverse applicazioni dello stesso fornitore.

    Selezionare questa opzione se si desidera aggiungere i dettagli del certificato di un file eseguibile alle regole della categoria. Se il file eseguibile non dispone di alcun certificato, verrà ignorato. Nessuna informazione sul file verrà aggiunta alla categoria.

  - Solo SHA-256 (i file senza hash verranno ignorati)

    Ogni file dispone di una specifica funzione hash SHA256 univoca. Quando si seleziona una funzione hash SHA256, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

    Selezionare questa opzione se si desidera aggiungere solo i dettagli della funzione hash SHA256 del file eseguibile.

  - Solo MD5 (modalità non più disponibile, solo per Kaspersky Endpoint Security 10 versione Service Pack 1)

Selezionare questa opzione solo se si utilizza Kaspersky Endpoint Security for Windows. Kaspersky Endpoint Security for Linux non supporta una funzione hash MD5.

Ogni file dispone di una specifica funzione hash MD5 univoca. Quando si seleziona una funzione hash MD5, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

5. Fare clic su **OK**.

Al termine della procedura guidata, i file eseguibili relativi agli eventi di Controllo Applicazioni vengono aggiunti alla categoria di applicazioni esistente o a una nuova categoria di applicazioni. È possibile visualizzare le impostazioni della categoria di applicazioni che è stata modificata o creata.

Per informazioni dettagliate su Controllo Applicazioni, consultare la Guida di Kaspersky Endpoint Security for Linux e la Guida di Kaspersky Endpoint Security for Windows.

Guida di riferimento API

Questa guida di riferimento di Kaspersky Security Center OpenAPI è progettata per assistere nelle seguenti attività:

- Automazione e personalizzazione. È possibile automatizzare le attività che è preferibile non gestire manualmente. Come amministratore è ad esempio possibile utilizzare Kaspersky Security Center OpenAPI per creare ed eseguire script che faciliteranno lo sviluppo della struttura dei gruppi di amministrazione e manterranno aggiornata tale struttura.

- Sviluppo personalizzato. Usando OpenAPI, è possibile sviluppare un'applicazione client.

È possibile utilizzare il campo di ricerca nella parte destra dello schermo per individuare le informazioni necessarie nella guida di riferimento OpenAPI.

GUIDA DI RIFERIMENTO OPENAPI

Esempi di script

La guida di riferimento OpenAPI contiene gli esempi di script Python elencati nella tabella seguente. Gli esempi mostrano come chiamare i metodi OpenAPI ed eseguire automaticamente varie attività per proteggere la rete, ad esempio creare una gerarchia di tipo "primario/secondario", eseguire attività in Kaspersky Security Center Linux o assegnare punti di distribuzione. È possibile eseguire gli esempi così come sono o creare script personalizzati basati sugli esempi.

Per chiamare i metodi OpenAPI ed eseguire gli script:

1. Scaricare l'archivio KlAkOAPI.tar.gz. Questo archivio include il pacchetto KlAkOAPI e gli esempi (è possibile copiarli dall'archivio o dalla guida di riferimento OpenAPI). L'archivio KlAkOAPI.tar.gz si trova anche nella cartella di installazione di Kaspersky Security Center Linux.

2. Installare il pacchetto KlAkOAPI dall'archivio KlAkOAPI.tar.gz in un dispositivo in cui è installato Administration Server.

   È possibile chiamare i metodi OpenAPI, eseguire gli esempi e gli script personalizzati solo nei dispositivi in cui sono installati Administration Server e il pacchetto KlAkOAPI.

Corrispondenza tra scenari utente ed esempi di metodi Kaspersky Security Center OpenAPI

Esempio	Finalità dell'esempio	Scenario
Registro KlAkParams	È possibile estrarre ed elaborare i dati utilizzando la struttura di dati `KlAkParams`. L'esempio mostra come utilizzare questa struttura di dati. Il risultato dell'esempio può presentarsi in diversi modi. È possibile ottenere i dati per inviare un metodo HTTP o per utilizzarlo nel proprio codice.	Monitoraggio e generazione dei rapporti
Creazione ed eliminazione di una gerarchia "primaria/secondaria"	È possibile aggiungere un Administration Server secondario e stabilire una gerarchia "primaria/secondaria". In alternativa, è possibile disconnettere l'Administration Server secondario dalla gerarchia.	Creazione di una gerarchia di Administration Server, aggiunta di un Administration Server secondario ed eliminazione di una gerarchia di Administration Server
Scaricare i file dell'elenco di reti tramite il gateway di connessione nell'host specificato	È possibile connettersi a Network Agent nel dispositivo necessario utilizzando un gateway di connessione, quindi scaricare un file con l'elenco di reti nel dispositivo.	Regolazione di punti di distribuzione e gateway di connessione
Installazione di una chiave di licenza archiviata nell'archivio primario dell'Administration	È possibile connettersi all'Administration Server primario, scaricare una chiave di licenza richiesta da questo e trasmettere tale chiave a tutti gli Administration Server secondari inclusi in una gerarchia.	Licensing delle applicazioni gestite

Server sugli Administration Server secondari		
Creare un rapporto dei diritti utente effettivi	È possibile creare diversi rapporti. È ad esempio possibile generare il rapporto dei diritti utente effettivi utilizzando questo esempio. Questo rapporto descrive i diritti di cui dispone un utente, a seconda del relativo gruppo e ruolo. È possibile scaricare il rapporto in formato HTML, PDF o Excel.	Generazione e visualizzazione di un rapporto
Avvio dell'attività del dispositivo	È possibile connettersi a Network Agent nel dispositivo necessario utilizzando un gateway di connessione, quindi eseguire l'attività necessaria.	Avvio manuale di un'attività
Registrare i punti di distribuzione per i dispositivi in un gruppo	È possibile assegnare dispositivi gestiti come punti di distribuzione (precedentemente noti come Update Agent).	Aggiornamento di database e applicazioni Kaspersky
Enumerare tutti i gruppi	È possibile eseguire varie azioni con i gruppi di amministrazione. L'esempio mostra come effettuare le seguenti operazioni: • Ottenere un identificatore del gruppo radice "Dispositivi gestiti" • Spostarsi nella gerarchia dei gruppi • Recuperare la gerarchia completa ed estesa dei gruppi, insieme ai relativi nomi e livelli di nidificazione	Configurazione di Administration Server
Enumerare le attività, eseguire query sulle statistiche delle attività ed eseguire un'attività	È possibile trovare le seguenti informazioni: • Cronologia dell'avanzamento dell'attività • Stato dell'attività corrente • Numero di attività con diversi stati È inoltre possibile eseguire un'attività. Per impostazione predefinita, l'esempio esegue un'attività dopo aver generato le statistiche.	Gestione di attività
Creare ed eseguire un'attività	È possibile creare un'attività. Specificare i seguenti parametri dell'attività nell'esempio: • Tipo • Metodo di esecuzione • Nome • Gruppo di dispositivi per cui verrà utilizzata l'attività Per impostazione predefinita, l'esempio crea un'attività con il tipo "Mostra messaggio". È possibile eseguire questa attività per tutti i dispositivi gestiti di Administration Server. Se necessario, è possibile specificare i propri parametri dell'attività.	Creazione di un'attività
Enumerare le chiavi di licenza	È possibile ottenere un elenco di tutte le chiavi di licenza attive per le applicazioni Kaspersky installate nei dispositivi gestiti di Administration Server. L'elenco contiene dati dettagliati su ogni chiave di licenza, tra cui nome, tipo o data di scadenza.	Visualizzazione delle informazioni sulle chiavi di licenza in uso
Creare e trovare un utente interno	È possibile creare un account per utilizzi successivi.	Aggiunta di un account di un utente interno
Creare una categoria personalizzata	È possibile creare la categoria di applicazioni con i parametri necessari.	Creazione di una categoria di applicazioni con contenuto aggiunto manualmente
Enumerare gli utenti utilizzando SrvView	È possibile utilizzare la classe SrvView per richiedere informazioni dettagliate da Administration Server. È ad esempio possibile ottenere un elenco di utenti utilizzando questo esempio.	Gestione di utenti e ruoli utente

Applicazioni che interagiscono con Kaspersky Security Center Linux tramite OpenAPI

Alcune applicazioni interagiscono con Kaspersky Security Center Linux tramite OpenAPI. Tra queste applicazioni sono incluse, ad esempio, Kaspersky Anti Targeted Attack Platform o Kaspersky Security for Virtualization. Può anche trattarsi di un'applicazione client personalizzata sviluppata dall'utente su OpenAPI.

Le applicazioni che interagiscono con Kaspersky Security Center Linux tramite OpenAPI si connettono ad Administration Server. Se è stato configurato un elenco di indirizzi IP consentiti per la connessione ad Administration Server, aggiungere gli indirizzi IP dei dispositivi in cui sono installate le applicazioni che utilizzano Kaspersky Security Center Linux OpenAPI. Per scoprire se l'applicazione in uso funziona con OpenAPI, vedere la Guida di tale applicazione.

Procedure consigliate per i provider di servizi

Questa sezione fornisce informazioni su come configurare e utilizzare Kaspersky Security Center Linux.

Questa sezione contiene raccomandazioni relative alla distribuzione, alla configurazione e all'utilizzo dell'applicazione e descrive come risolvere i problemi più comuni che possono verificarsi durante l'esecuzione dell'applicazione.

Pianificazione della distribuzione di Kaspersky Security Center Linux

Durante la pianificazione della distribuzione dei componenti di Kaspersky Security Center Linux nella rete di un'organizzazione, è necessario tenere conto delle dimensioni e dell'ambito del progetto, in particolare per quanto riguarda i seguenti fattori:

- Numero totale di dispositivi
- Numero di client MSP

Un solo Administration Server può supportare un massimo di 50.000 dispositivi. Se il numero totale di dispositivi nella rete di un'organizzazione è superiore a 50.000, il provider di servizi deve distribuire più Administration Server, che possono essere combinati in una gerarchia per gestirli comodamente in modo centralizzato.

È possibile creare fino a 500 Server virtuali in un singolo Administration Server, pertanto è richiesto un singolo Administration Server ogni 500 client MSP.

In fase di pianificazione della distribuzione, deve essere valutata l'assegnazione di uno speciale certificato X.509 all'Administration Server. L'assegnazione del certificato X.509 all'Administration Server può essere utile nei seguenti casi (elenco parziale):

- Ispezione del traffico SSL (Secure Sockets Layer) per mezzo di un proxy con terminazione SSL
- Specificazione dei valori richiesti nei campi del certificato
- Specificazione del livello di criptaggio richiesto di un certificato

Concessione dell'accesso via Internet all'Administration Server

Per consentire ai dispositivi nella rete client di accedere ad Administration Server via Internet, è necessario rendere disponibili le seguenti porte di Administration Server:

- TCP 13000: porta TLS di Administration Server per la connessione dei Network Agent distribuiti nella rete client
- TCP 8061: porta HTTPS per la pubblicazione dei pacchetti indipendenti utilizzando gli strumenti di Kaspersky Security Center Web Console
- TCP 8060: porta HTTP per la pubblicazione dei pacchetti indipendenti utilizzando gli strumenti di Kaspersky Security Center Web Console
- TCP 13292: porta TLS necessaria solo se sono presenti dispositivi mobili da gestire
- TCP 8080: porta HTTPS per Kaspersky Security Center Web Console

Configurazione standard di Kaspersky Security Center Linux

Uno o più Administration Server vengono distribuiti nei server degli MSP. Il numero di Administration Server che è possibile selezionare può essere basato sull'hardware disponibile, sul numero totale di client MSP gestiti o sul numero totale di dispositivi gestiti.

Un solo Administration Server può supportare fino a 50.000 dispositivi. È necessario tenere conto della possibilità di aumentare il numero di dispositivi gestiti in futuro: può essere utile connettere un numero più limitato di dispositivi a un singolo Administration Server.

È possibile creare fino a 500 Server virtuali in un singolo Administration Server, pertanto è richiesto un singolo Administration Server ogni 500 client MSP.

Se vengono utilizzati più server, è consigliabile combinarli in una gerarchia. L'utilizzo di una gerarchia di Administration Server consente di evitare la duplicazione di criteri e attività e di amministrare l'intero set di dispositivi gestiti come se fossero gestiti da un singolo Administration Server (ricerca di dispositivi, creazione di selezioni di dispositivi e generazione di rapporti).

In ogni server virtuale corrispondente a un client MSP è necessario assegnare uno o più punti di distribuzione. Se i client MSP e Administration Server sono collegati via Internet, può essere utile creare un'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per i punti di distribuzione, in modo che scarichino gli aggiornamenti direttamente dai server di Kaspersky, invece che da Administration Server.

Se alcuni dispositivi della rete client MSP non hanno accesso diretto a Internet, è necessario attivare la modalità gateway di connessione per i punti di distribuzione. In questo caso, i Network Agent nei dispositivi nella rete del client MSP saranno connessi per l'ulteriore sincronizzazione ad Administration Server, ma attraverso il gateway, non direttamente.

Poiché in genere Administration Server non è in grado di eseguire il polling della rete del client MSP, può essere utile assegnare questa funzione a un punto di distribuzione.

Administration Server non potrà inviare notifiche tramite la porta UDP 15000 ai dispositivi gestiti posizionati dietro il NAT nella rete del client MSP. Per risolvere questo problema, può essere utile abilitare la modalità di connessione continua ad Administration Server nelle proprietà dei dispositivi che operano come punti di distribuzione e vengono eseguiti in modalità gateway di connessione (opzione **Non eseguire la disconnessione da Administration Server**). La modalità di connessione continua è disponibile se il numero totale di punti di distribuzione non è superiore a 300.

Un client MSP potrebbe voler gestire i dispositivi Android e i dispositivi iOS dei dipendenti. Administration Server gestisce i dispositivi mobili tramite TLS, porta TCP 13292.

Informazioni sui punti di distribuzione

Il dispositivo in cui è installato Network Agent può essere utilizzato come punto di distribuzione. In questa modalità, Network Agent può eseguire le seguenti funzioni:

- Trasferire file ai dispositivi client, tra cui:
  - Aggiornamenti dei moduli software e database Kaspersky

    Gli aggiornamenti possono essere recuperati dall'Administration Server o dai server di Kaspersky. Nel secondo caso, è necessario creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per il dispositivo che opera come punto di distribuzione.

- Aggiornamenti software di terze parti
- Pacchetti di installazione

- Installare il software (inclusa la distribuzione iniziale dei Network Agent) in altri dispositivi.
- Eseguire il polling della rete per rilevare nuovi dispositivi e aggiornare le informazioni sui dispositivi esistenti. Un punto di distribuzione può applicare gli stessi metodi di device discovery di Administration Server.

La distribuzione dei punti di distribuzione nella rete di un'organizzazione ha i seguenti obiettivi:

- Ridurre il carico su Administration Server se questo opera come sorgente degli aggiornamenti.
- Ottimizzare il traffico Internet poiché, in questo caso, ogni dispositivo nella rete del client MSP non deve accedere ai server di Kaspersky o ad Administration Server per gli aggiornamenti.
- Concedere l'accesso ad Administration Server ai dispositivi dietro il NAT (rispetto ad Administration Server) della rete del client MSP, consentendo ad Administration Server di eseguire le seguenti azioni:
  - Inviare notifiche ai dispositivi tramite UDP nella rete IPv4 o IPv6
  - Eseguire il polling della rete IPv4 o IPv6
  - Eseguire la distribuzione iniziale
  - Fungere da server push

Un punto di distribuzione viene assegnato a un gruppo di amministrazione. In questo caso, l'ambito del punto di distribuzione include tutti i dispositivi contenuti nel gruppo di amministrazione e in tutti i relativi sottogruppi. Tuttavia, il dispositivo che opera come punto di distribuzione può non essere incluso nel gruppo di amministrazione a cui è stato assegnato.

È possibile far funzionare un punto di distribuzione come gateway di connessione. In questo caso, i dispositivi nell'ambito del punto di distribuzione saranno connessi all'Administration Server tramite il gateway, non direttamente. È possibile utilizzare questa modalità negli scenari che non consentono di stabilire una connessione diretta tra i dispositivi con Network Agent e un Administration Server.

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Gerarchia di Administration Server

Alcune società clienti, ad esempio MSP, possono eseguire più Administration Server. Poiché può essere scomodo amministrare più Administration Server distinti, è possibile applicare una gerarchia. In una gerarchia, un Administration Server basato su Linux può fungere sia da server primario che da server secondario. Il server primario basato su Linux può gestire sia i server secondari basati su Linux che quelli basati su Windows. Un server primario basato su Windows può gestire un server secondario basato su Linux.

Una configurazione "primario/secondario" per due Administration Server fornisce le seguenti opzioni:

- Un Administration Server secondario eredita i criteri, le attività, i ruoli utente e i pacchetti di installazione dall'Administration Server primario, evitando così la duplicazione delle impostazioni.

- Le selezioni di dispositivi nell'Administration Server primario possono includere i dispositivi degli Administration Server secondari.
- I rapporti nell'Administration Server primario possono contenere dati (incluse informazioni dettagliate) ottenuti dagli Administration Server secondari.
- È possibile utilizzare un Administration Server primario come sorgente degli aggiornamenti per l'Administration Server secondario.

L'Administration Server primario riceve i dati solo dagli Administration Server secondari non virtuali nell'ambito delle opzioni elencate sopra. Questa limitazione non si applica agli Administration Server virtuali, che condividono il database con l'Administration Server primario.

Administration Server virtuali

Sulla base di un Administration Server fisico, è possibile creare più Administration Server virtuali, simili agli Administration Server secondari. Rispetto al modello di accesso discrezionale, che è basato su elenchi di controllo di accesso (ACL), il modello degli Administration Server virtuali è più funzionale e fornisce un maggior livello di isolamento. Oltre a una struttura dedicata di gruppi di amministrazione per i dispositivi assegnati con criteri e attività, ogni Administration Server virtuale dispone di un proprio gruppo di dispositivi non assegnati, di insiemi di rapporti, dispositivi ed eventi selezionati, pacchetti di installazione, regole di spostamento e così via. Per il massimo isolamento reciproco dei client MSP, è consigliabile scegliere Administration Server virtuali come funzionalità da utilizzare. Inoltre, la creazione di un Administration Server virtuale per ogni client MSP consente di offrire ai client opzioni di base per l'amministrazione della rete tramite Kaspersky Security Center Web Console.

Gli Administration Server virtuali sono molto simili agli Administration Server secondari, ma con le seguenti distinzioni:

- Un Administration Server virtuale non dispone della maggior parte delle impostazioni globali e di specifiche porte TCP.
- Un Administration Server virtuale non dispone di Administration Server secondari.
- Un Administration Server virtuale non include altri Administration Server virtuali.
- Un Administration Server fisico visualizza i dispositivi, i gruppi, gli eventi e gli oggetti nei dispositivi gestiti (elementi in Quarantena, registro delle applicazioni e così via) di tutti i relativi Administration Server virtuali.
- Un Administration Server virtuale può eseguire solo la scansione della rete a cui sono connessi punti di distribuzione.

Distribuzione e configurazione iniziale

Kaspersky Security Center Linux è un'applicazione distribuita. Kaspersky Security Center Linux include le seguenti applicazioni:

- Administration Server - Il componente principale, progettato per la gestione dei dispositivi di un'organizzazione e l'archiviazione dei dati in un sistema DBMS.
- Kaspersky Security Center Web Console — Un'interfaccia Web per Administration Server pensata per le operazioni di base. È possibile installare il componente in qualsiasi dispositivo che soddisfi i requisiti hardware e software.

- Network Agent: utilizzato per gestire l'applicazione di protezione installata in un dispositivo, nonché per ottenere informazioni sul dispositivo. I Network Agent vengono installati nei dispositivi di un'organizzazione.

La distribuzione di Kaspersky Security Center Linux nella rete di un'organizzazione viene eseguita come segue:

- Installazione di Administration Server
- Installazione di Kaspersky Security Center Web Console
- Installazione di Network Agent e dell'applicazione di protezione nei dispositivi dell'organizzazione

Raccomandazioni sull'installazione di Administration Server

Questa sezione contiene raccomandazioni su come installare Administration Server. Vengono inoltre illustrati gli scenari per l'utilizzo di una cartella condivisa nel dispositivo con Administration Server per distribuire Network Agent nei dispositivi client.

Creazione degli account per i servizi di Administration Server in un cluster di failover

Prima di iniziare la distribuzione di Kaspersky Security Center Linux su un cluster di failover, è necessario creare account per i servizi Kaspersky Security Center Linux.

A tale scopo, effettuare le seguenti operazioni sul nodo attivo, sul nodo passivo e sul file server:

1. Creare un gruppo con il nome "kladmins" e assegnare lo stesso GID a tutti e tre i gruppi.
2. Creare un account utente con il nome "ksc" e assegnare lo stesso UID a tutti e tre gli account utente. Impostare il gruppo primario su "kladmins" per gli account creati.
3. Creare un account utente con il nome "rightless" e assegnare lo stesso UID a tutti e tre gli account utente. Impostare il gruppo primario su "kladmins" per gli account creati.

Selezione di un DBMS

Nella seguente tabella, sono elencate le opzioni DBMS valide, nonché i suggerimenti e le limitazioni per il relativo utilizzo.

Suggerimenti e limitazioni su DBMS

DBMS	Suggerimenti e limitazioni
MySQL (vedere le versioni supportate)	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 20.000 dispositivi.
MariaDB (vedere le versioni supportate)	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 20.000 dispositivi.
PostgreSQL, Postgres Pro (vedere le versioni supportate)	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 50.000 dispositivi.

Per informazioni su come installare il DBMS selezionato, consultare la relativa documentazione.

Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate.

Se si decide di installare il DBMS di PostgreSQL o Postgres Pro, assicurarsi di aver specificato una password per il l'utente con privilegi avanzati. Se la password non viene specificata, Administration Server potrebbe non essere in grado di connettersi al database.

Se si installa MySQL, MariaDB, PostgreSQL o Postgres Pro, utilizzare le impostazioni consigliate per garantire il corretto funzionamento del DBMS.

Se si utilizza un DBMS PostgreSQL, MariaDB o MySQL, la scheda **Eventi** potrebbe mostrare un elenco incompleto di eventi per il dispositivo client selezionato. Questo si verifica quando il DBMS archivia una quantità molto elevata di eventi. È possibile aumentare il numero di eventi visualizzati effettuando una delle seguenti operazioni:

- Rimozione degli eventi non necessari.
- Riduzione del periodo di archiviazione per gli eventi non necessari.

Per visualizzare un elenco completo degli eventi registrati in Administration Server per il dispositivo, utilizzare Rapporti.

Specificazione dell'indirizzo dell'Administration Server

Durante l'installazione di Administration Server, è necessario specificare l'indirizzo IP statico o il nome DNS di Administration Server. Questo indirizzo sarà utilizzato come indirizzo predefinito al momento della creazione dei pacchetti di installazione di Network Agent. Sarà quindi possibile modificare l'indirizzo dell'host di Administration Server utilizzando gli strumenti di Kaspersky Security Center Web Console. L'indirizzo non sarà modificato automaticamente nei pacchetti di installazione di Network Agent che sono stati già creati.

Distribuzione di Network Agent e delle applicazioni di protezione

Per gestire i dispositivi di un'organizzazione e proteggerli dalle minacce alla sicurezza, è necessario installare Network Agent e un'applicazione di protezione Kaspersky su ciascuno di essi.

Per informazioni sulla distribuzione della protezione, fare riferimento alla sezione Distribuzione di Network Agent e dell'applicazione di protezione.

In Microsoft Windows XP, Network Agent potrebbe non eseguire correttamente le seguenti operazioni: scaricare gli aggiornamenti direttamente dai server Kaspersky (come punto di distribuzione) e funzionare come server proxy KSN (come punto di distribuzione).

Configurazione della protezione nella rete di un'organizzazione client

Al termine dell'installazione di Administration Server, Kaspersky Security Center Web Console viene avviato e richiede di eseguire la configurazione iniziale tramite la procedura guidata appropriata. Durante l'esecuzione dell'Avvio rapido guidato, i seguenti criteri e attività vengono creati nel gruppo di amministrazione radice:

- Criterio di Kaspersky Endpoint Security
- Attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
- Attività di gruppo per la scansione di un dispositivo con Kaspersky Endpoint Security
- Criterio di Network Agent
- Attività Scansione vulnerabilità (attività di Network Agent)
- Attività di installazione degli aggiornamenti e correzione delle vulnerabilità (attività di Network Agent)

I criteri e le attività sono creati con le impostazioni predefinite, che possono risultare non ottimali o perfino non utilizzabili per l'organizzazione. È pertanto necessario verificare le proprietà degli oggetti che sono stati creati e modificarle manualmente, se necessario.

Questa sezione contiene informazioni sulla configurazione manuale di criteri, attività e altre impostazioni di Administration Server, nonché le informazioni sul punto di distribuzione, sulla creazione di una struttura di gruppi di amministrazione e di una gerarchia di attività e altre impostazioni.

Configurazione manuale del criterio di Kaspersky Endpoint Security

Questa sezione fornisce raccomandazioni su come configurare il criterio di Kaspersky Endpoint Security, creato dall'Avvio rapido guidato. È possibile eseguire la configurazione nella finestra delle proprietà del criterio.

Quando si modifica un'impostazione, tenere presente che è possibile bloccarla o sbloccarla per impedirne o consentirne la modifica del valore in una workstation.

Configurazione del criterio nella sezione Protezione minacce avanzata

Per una descrizione completa delle impostazioni in questa sezione, fare riferimento alla documentazione di Kaspersky Endpoint Security for Windows.

Nella sezione **Protezione minacce avanzata** è possibile configurare l'utilizzo di Kaspersky Security Network per Kaspersky Endpoint Security for Windows. È inoltre possibile configurare i moduli di Kaspersky Endpoint Security for Windows, ad esempio Rilevamento del Comportamento, Prevenzione Exploit, Prevenzione Intrusioni Host e Motore di Remediation.

Nella sottosezione **Kaspersky Security Network** è consigliabile abilitare l'opzione **Kaspersky Security Network**. L'utilizzo di questa opzione consente di ridistribuire e ottimizzare il traffico nella rete. Se l'opzione **Kaspersky Security Network** è disabilitata, è possibile abilitare l'uso diretto dei server KSN.

Configurazione del criterio nella sezione Protezione minacce essenziale

Per una descrizione completa delle impostazioni in questa sezione, fare riferimento alla documentazione di Kaspersky Endpoint Security for Windows.

Nella sezione **Protezione minacce essenziale** della finestra delle proprietà del criterio, si consiglia di specificare impostazioni aggiuntive nelle sottosezioni **Firewall** e **Protezione minacce file**.

La sottosezione **Firewall** contiene le impostazioni che consentono di controllare le attività di rete delle applicazioni sui dispositivi client. Un dispositivo client utilizza una rete a cui è assegnato uno dei seguenti stati: pubblico, locale o attendibile. A seconda dello stato della rete, Kaspersky Endpoint Security può consentire o negare le attività di rete su un dispositivo. Quando si aggiunge una nuova rete all'organizzazione, è necessario assegnare uno stato di rete appropriato a questa. Ad esempio, se il dispositivo client è un laptop, si consiglia che questo dispositivo utilizzi la rete pubblica o attendibile, poiché il laptop non è sempre connesso alla rete locale. Nella sottosezione **Firewall**, è possibile verificare se sono stati assegnati correttamente gli stati alle reti utilizzate nell'organizzazione.

Per controllare l'elenco delle reti:

1. Nelle proprietà del criterio, passare a **Protezione minacce essenziale** → **Firewall**.
2. Nella sezione **Reti disponibili**, fare clic sul pulsante **Impostazioni**.
3. Nella finestra **Firewall** visualizzata, passare alla scheda **Reti** per visualizzare l'elenco delle reti.

Nella sottosezione **Protezione minacce file**, è possibile disabilitare la scansione delle unità di rete. La scansione delle unità di rete può comportare un carico significativo per le unità di rete. È più pratico eseguire la scansione indiretta sui file server.

Per disabilitare la scansione delle unità di rete:

1. Nelle proprietà del criterio, passare a **Protezione minacce essenziale** → **Protezione minacce file**.
2. Nella sezione **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
3. Nella finestra **Protezione minacce file** visualizzata, nella scheda **Generali**, deselezionare la casella di controllo **Tutte le unità di rete**.

Configurazione del criterio nella sezione Impostazioni generali

Per la descrizione completa delle impostazioni in questa sezione, fare riferimento alla documentazione di Kaspersky Endpoint Security.

Di seguito sono descritte le operazioni di configurazione avanzate che è consigliabile eseguire nella sezione **Impostazioni generali** della finestra delle proprietà del criterio di Kaspersky Endpoint Security.

Sezione Impostazioni generali, sottosezione Rapporti e archivi

Nella sezione **Trasferimento dei dati ad Administration Server**, notare la casella di controllo **Informazioni sulle applicazioni avviate**. Se questa casella di controllo è selezionata, il database di Administration Server salva informazioni su tutte le versioni di tutti i moduli software nei dispositivi connessi alla rete. Queste informazioni possono richiedere una quantità significativa di spazio su disco nel database di Kaspersky Security Center Linux (decine di gigabyte). Pertanto, se la casella di controllo **Informazioni sulle applicazioni avviate** è ancora selezionata nel criterio di primo livello, deve essere deselezionata.

Sezione Impostazioni generali, sottosezione Interfaccia

Se la protezione dalle minacce nella rete dell'organizzazione deve essere gestita in modalità centralizzata tramite Kaspersky Security Center Web Console, è necessario disabilitare la visualizzazione dell'interfaccia di utente di Kaspersky Endpoint Security nelle workstation (deselezionando la casella di controllo **Visualizza interfaccia applicazione** nella sezione **Interazione con l'utente**) e abilitare la protezione tramite password (selezionando la casella di controllo **Abilita la protezione tramite password** nella sezione **Protezione tramite password**).

Configurazione del criterio nella sezione Configurazione eventi

Nella sezione **Configurazione eventi** è consigliabile disabilitare il salvataggio di qualsiasi evento in Administration Server, tranne i seguenti:

- Nella scheda **Critico**:
  - *L'esecuzione automatica dell'applicazione è disabilitata*
  - *Accesso negato*
  - *Avvio dell'applicazione non consentito*
  - *Disinfezione non attuabile*
  - *Contratto di licenza con l'utente finale violato*
  - *Impossibile caricare il modulo di criptaggio*
  - *Impossibile avviare due attività contemporaneamente*
  - *È stata rilevata una minaccia attiva. Si consiglia di avviare Disinfezione avanzata*
  - *Attacco di rete rilevato*
  - *Non tutti i componenti sono stati aggiornati*
  - *Errore di attivazione*
  - *Errore durante l'abilitazione della modalità portatile*
  - *Errore durante l'interazione con Kaspersky Security Center*
  - *Errore durante la disabilitazione della modalità portatile*
  - *Errore durante la modifica dei componenti dell'applicazione*
  - *Errore durante l'applicazione delle regole di criptaggio/decriptaggio dei file*
  - *Il criterio non può essere applicato*
  - *Processo terminato*
  - *Attività di rete bloccata*
- Nella scheda **Errore funzionale**: *Impostazioni attività non valide. Impostazioni non applicate*
- Nella scheda **Avviso**:

- *L'Auto-difesa è disabilitata*
- *Chiave di riserva errata*
- *L'utente ha scelto di non applicare il criterio di criptaggio*

- Nella scheda **Informazioni**: *Avvio dell'applicazione non consentito in modalità di test*

Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security

Se Administration Server opera come sorgente degli aggiornamenti, l'opzione di pianificazione ottimale e consigliata per Kaspersky Endpoint Security è **Quando vengono scaricati nuovi aggiornamenti nell'archivio** con la casella di controllo **Usa automaticamente il ritardo casuale per l'avvio delle attività** selezionata.

Se si crea un'attività locale di download degli aggiornamenti dai server Kaspersky nell'archivio in ogni punto di distribuzione, la pianificazione periodica sarà ottimale e consigliata per l'attività di aggiornamento di gruppo di Kaspersky Endpoint Security. In questo caso, il valore dell'intervallo con impostazione casuale deve essere impostato su 1 ora.

Configurazione manuale dell'attività di gruppo per la scansione di un dispositivo con Kaspersky Endpoint Security

L'Avvio rapido guidato crea un'attività di gruppo per la scansione di un dispositivo. Se la pianificazione specificata automaticamente dell'attività di scansione di gruppo non è appropriata per l'organizzazione, è necessario impostare manualmente la pianificazione più adatta per questa attività in base alle regole del luogo di lavoro adottate nell'organizzazione.

Ad esempio, all'attività viene assegnata una pianificazione **Esegui il venerdì alle 19:00** con un'impostazione casuale automatica e la casella di controllo **Esegui attività non effettuate** è deselezionata. Di conseguenza, se i dispositivi nell'organizzazione vengono spenti ad esempio il venerdì alle 18:30, l'attività di scansione del dispositivo non verrà eseguita. In questo caso, è necessario impostare manualmente l'attività di scansione di gruppo.

Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti

L'Avvio rapido guidato crea l'attività *Trova vulnerabilità e aggiornamenti richiesti* per Network Agent. Per impostazione predefinita, all'attività viene assegnata una pianificazione **Esegui il martedì alle 19:00** con un'impostazione casuale automatica e la casella di controllo **Esegui attività non effettuate** è selezionata.

Se le regole dell'organizzazione per l'ambiente di lavoro prevedono lo spegnimento di tutti i dispositivi in tale orario, l'attività *Trova vulnerabilità e aggiornamenti richiesti* verrà eseguita dopo la riaccensione dei dispositivi, il mercoledì mattina. Un'attività di questo tipo potrebbe essere indesiderabile perché una Scansione vulnerabilità può aumentare il carico sui sottosistemi del disco e della CPU. È necessario impostare la pianificazione appropriata per l'attività in base alle regole per l'ambiente di lavoro adottate nell'organizzazione.

Configurazione manuale dell'attività di gruppo per l'installazione degli aggiornamenti e la correzione delle vulnerabilità

L'Avvio rapido guidato crea un'attività di gruppo per l'installazione degli aggiornamenti e la correzione delle vulnerabilità per Network Agent. Per impostazione predefinita, l'attività è impostata per l'esecuzione ogni giorno alle 01:00, con un'impostazione casuale automatica, e l'opzione **Esegui attività non effettuate** non è abilitata.

Se le regole dell'organizzazione per l'ambiente di lavoro prevedono lo spegnimento dei dispositivi durante la notte, l'installazione degli aggiornamenti non verrà eseguita. È necessario impostare la pianificazione appropriata per l'attività Scansione vulnerabilità in base alle regole per l'ambiente di lavoro adottate nell'organizzazione. È anche importante tenere presente che l'installazione degli aggiornamenti può richiedere il riavvio del dispositivo.

Creazione di una struttura di gruppi di amministrazione e assegnazione dei punti di distribuzione

Una struttura di gruppi di amministrazione in Kaspersky Security Center Linux esegue le seguenti funzioni:

- Imposta l'ambito dei criteri.

  È disponibile un metodo alternativo per l'applicazione delle impostazioni appropriate nei dispositivi, utilizzando i profili criterio. In questo caso, l'ambito dei criteri viene impostato, ad esempio, tramite tag dispositivo o ruoli utente.

- Imposta l'ambito delle attività di gruppo.

  Esiste un approccio alla definizione dell'ambito delle attività di gruppo che non è basato su una gerarchia di gruppi di amministrazione: l'utilizzo di attività per selezioni dispositivi e di attività per dispositivi specifici.

- Imposta i diritti di accesso a dispositivi, Administration Server virtuali e Administration Server secondari.

- Assegna i punti di distribuzione.

Al momento della creazione della struttura dei gruppi di amministrazione, è necessario tenere conto della topologia della rete dell'organizzazione per l'assegnazione ottimale dei punti di distribuzione. La distribuzione ottimale dei punti di distribuzione consente di ridurre il traffico nella rete dell'organizzazione.

A seconda dello schema dell'organizzazione e della topologia di rete adottata dal client MSP, le seguenti configurazioni standard possono essere applicate alla struttura dei gruppi di amministrazione:

- Singola sede

- Più sedi separate di piccole dimensioni

Configurazione del client MSP standard: singola sede

In una configurazione standard con una singola sede, tutti i dispositivi si trovano nella rete dell'organizzazione e sono visibili reciprocamente. La rete dell'organizzazione può comprendere diversi componenti (reti o segmenti di rete) connessi tramite canali con larghezza di banda ridotta.

Sono disponibili i seguenti metodi per creare la struttura dei gruppi di amministrazione:

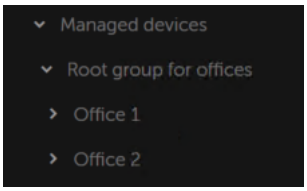
- Creazione della struttura dei gruppi di amministrazione tenendo conto della topologia di rete. La struttura dei gruppi di amministrazione potrebbe non riflettere la topologia di rete alla perfezione. Una corrispondenza tra i diversi componenti della rete e alcuni gruppi di amministrazione può essere sufficiente. È possibile utilizzare l'assegnazione automatica dei punti di distribuzione o assegnarli manualmente.

- Creazione della struttura dei gruppi di amministrazione senza tenere conto della topologia di rete. In questo caso è necessario disabilitare l'assegnazione automatica dei punti di distribuzione e quindi assegnare a uno o più dispositivi il ruolo di punti di distribuzione per un gruppo di amministrazione radice in ciascun componente della rete, ad esempio per il gruppo **Dispositivi gestiti**. Tutti i punti di distribuzione saranno allo stesso livello e avranno lo stesso ambito che comprende tutti i dispositivi della rete dell'organizzazione. In questo caso, tutti i Network Agent si connetteranno al punto di distribuzione con il percorso più vicino. Il percorso di un punto di distribuzione è monitorabile con l'utilità tracert o l'utilità traceroute.

Configurazione del client MSP standard: più sedi remote di piccole dimensioni

Questa configurazione standard prevede la presenza di diverse sedi remote, che possono comunicare con la sede centrale via Internet. Ogni sede remota è situata dietro il NAT, ovvero la connessione da una sede remota all'altra non è possibile perché le sedi sono isolate tra loro.

La configurazione deve essere riflessa nella struttura dei gruppi di amministrazione: è necessario creare un gruppo di amministrazione distinto per ogni sede remota (i gruppi **Sede 1** e **Sede 2** nella figura seguente).



Le sedi remote sono incluse nella struttura dei gruppi di amministrazione

È necessario assegnare uno o più punti di distribuzione a ogni gruppo di amministrazione che corrisponde a una sede. I punti di distribuzione devono essere dispositivi nella sede remota con una quantità sufficiente di spazio libero su disco. I dispositivi distribuiti nel gruppo **Sede 1**, ad esempio, accederanno ai punti di distribuzione assegnati al gruppo di amministrazione **Sede 1**.

Se alcuni utenti si spostano fisicamente tra le sedi con i loro computer portatili, è necessario selezionare due o più dispositivi (oltre ai punti di distribuzione esistenti) in ogni sede remota e assegnare loro il ruolo di punti di distribuzione per un gruppo di amministrazione di primo livello (**Gruppo radice per le sedi** nella figura precedente).

Esempio: un computer portatile è distribuito nel gruppo di amministrazione **Sede 1** e quindi viene spostato fisicamente nella sede che corrisponde al gruppo di amministrazione **Sede 2**. Dopo lo spostamento del portatile, Network Agent tenta di accedere ai punti di distribuzione assegnati al gruppo **Sede 1**, ma tali punti di distribuzione non sono disponibili. Network Agent inizia quindi a tentare di accedere ai punti di distribuzione che sono stati assegnati al **Gruppo radice per le sedi**. Poiché le sedi remote sono isolate tra loro, i tentativi di accedere ai punti di distribuzione assegnati al gruppo di amministrazione **Gruppo radice per le sedi** avranno esito positivo solo quando Network Agent tenta di accedere ai punti di distribuzione nel gruppo **Sede 2**. In altre parole, il computer portatile rimarrà nel gruppo di amministrazione che corrisponde alla sede iniziale, ma utilizzerà il punto di distribuzione della sede in cui si trova fisicamente al momento.

Gerarchia di criteri tramite i profili criterio

Questa sezione fornisce informazioni su come applicare i criteri ai dispositivi nei gruppi di amministrazione. Questa sezione fornisce anche informazioni sui profili dei criteri.

Gerarchia dei criteri

In Kaspersky Security Center Linux i criteri vengono utilizzati per definire una singola raccolta di impostazioni per più dispositivi. Ad esempio, l'ambito del criterio dell'applicazione P definito per il gruppo di amministrazione G include i dispositivi gestiti in cui è installata l'applicazione P che sono stati distribuiti nel gruppo G e in tutti i relativi sottogruppi, ad eccezione dei sottogruppi in cui la casella di controllo **Eredita da gruppo padre** è deselezionata nelle proprietà.

Un criterio differisce da qualsiasi impostazione locale in base alle icone di blocco (🔒) accanto alle relative impostazioni. Se un'impostazione (o un gruppo di impostazioni) è bloccata nelle proprietà del criterio, è necessario in primo luogo utilizzare questa impostazione (o gruppo di impostazioni) durante la creazione delle impostazioni da applicare e, in secondo luogo, scrivere le impostazioni o il gruppo di impostazioni nel criterio downstream.

La creazione delle impostazioni da applicare in un dispositivo può essere descritta come segue: i valori di tutte le impostazioni che non sono state bloccate vengono ottenuti dal criterio, quindi sono sovrascritti con i valori delle impostazioni locali. La raccolta risultante viene quindi sovrascritta con i valori delle impostazioni bloccate ottenuti dal criterio.

I criteri della stessa applicazione si influenzano reciprocamente attraverso la gerarchia dei gruppi di amministrazione: le impostazioni bloccate del criterio upstream sovrascrivono le stesse impostazioni del criterio downstream.

Esiste un criterio speciale per gli utenti fuori sede. Questo criterio ha effetto su un dispositivo quando il dispositivo passa in modalità fuori sede. I criteri fuori sede non influiscono sugli altri criteri attraverso la gerarchia dei gruppi di amministrazione.

Profili criterio

L'applicazione dei criteri ai dispositivi solo tramite la gerarchia dei gruppi di amministrazione in molte circostanze può essere poco pratica. Può essere necessario creare più istanze di un singolo criterio con una o due impostazioni differenti per gruppi di amministrazione diversi e sincronizzare i contenuti di questi criteri in futuro.

Per contribuire a evitare tali problemi, Kaspersky Security Center Linux supporta *profili di criteri*. Un profilo criterio è un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita *condizione di attivazione del profilo*. I profili contengono solo le impostazioni diverse dal criterio "di base" che è attivo sul dispositivo client (computer o dispositivo mobile). L'attivazione di un profilo determina la modifica delle impostazioni del criterio attivo nel dispositivo prima dell'attivazione del profilo. Tali impostazioni assumono i valori specificati nel profilo.

Attualmente ai profili criterio si applicano le seguenti limitazioni:

- Un criterio può includere al massimo 100 profili.
- Un profilo criterio non può contenere altri profili.
- Un profilo criterio non può contenere impostazioni di notifica.

Contenuto di un profilo

Un profilo criterio contiene i seguenti elementi:

- Nome. I profili con nomi identici si influenzano reciprocamente attraverso la gerarchia dei gruppi di amministrazione con regole comuni.

- Sottoinsieme di impostazioni dei criteri. A differenza del criterio, che contiene tutte le impostazioni, un profilo contiene solo le impostazioni che sono effettivamente richieste (le impostazioni bloccate).
- Condizione di attivazione è un'espressione logica con le proprietà del dispositivo. Un profilo è attivo (integra il criterio) solo quando la condizione di attivazione del profilo diventa vera. In tutti gli altri casi, il profilo è inattivo e viene ignorato. Le seguenti proprietà del dispositivo possono essere incluse nell'espressione logica:
  - Stato della modalità fuori sede.
  - Proprietà dell'ambiente di rete - Nome della regola attiva per la connessione di Network Agent.
  - Presenza o assenza dei tag specificati nel dispositivo.
  - Posizione del dispositivo in un'unità di Active Directory: esplicita (il dispositivo è direttamente nell'unità organizzativa specificata) o implicita (il dispositivo è in un'unità organizzativa che è contenuta nell'unità organizzativa specificata a qualsiasi livello di annidamento).
  - Appartenenza del dispositivo a un gruppo di protezione di Active Directory (esplicita o implicita).
  - Appartenenza del proprietario del dispositivo a un gruppo di protezione di Active Directory (esplicita o implicita).
- Casella di controllo per la disabilitazione del profilo. I profili disabilitati vengono sempre ignorati e le relative condizioni di attivazione non sono verificate.
- Priorità del profilo. Le condizioni di attivazione di differenti profili sono indipendenti, quindi è possibile attivare contemporaneamente più profili. Se i profili attivi contengono raccolte di impostazioni che non si sovrappongono, non si verifica alcun problema. Se invece due profili attivi contengono valori diversi della stessa impostazione, si verifica un'ambiguità. Questa ambiguità deve essere evitata tramite le priorità dei profili: il valore della variabile ambigua viene ottenuto dal profilo che ha la priorità più alta (quello al livello superiore nell'elenco dei profili).

Comportamento dei profili quando i criteri si influenzano reciprocamente attraverso la gerarchia

I profili con lo stesso nome vengono uniti in base alle regole di unione dei criteri. I profili di un criterio upstream hanno una priorità più alta rispetto ai profili di un criterio downstream. Se la modifica delle impostazioni non è consentita nel criterio upstream (è bloccata), il criterio downstream utilizza le condizioni di attivazione del profilo di quello upstream. Se la modifica delle impostazioni è consentita nel criterio upstream, vengono utilizzate le condizioni di attivazione del profilo del criterio downstream.

Poiché un profilo criterio può contenere la proprietà **Il dispositivo è offline** nella relativa condizione di attivazione, i profili sostituiscono completamente la funzionalità dei criteri per gli utenti fuori sede, che non saranno non più supportati.

Un criterio per gli utenti fuori sede può contenere profili, ma questi profili possono essere attivati solo una volta che il dispositivo passa alla modalità fuori sede.

Attività

Kaspersky Security Center Linux consente di gestire le applicazioni di protezione Kaspersky installate nei dispositivi creando ed eseguendo *attività*. Le attività sono necessarie per l'installazione, l'avvio e l'arresto delle applicazioni, la scansione dei file, l'aggiornamento dei database e dei moduli software, oltre che per eseguire altre azioni sulle applicazioni.

Le attività per un'applicazione specifica possono essere create solo se è installato il plug-in di gestione per tale applicazione.

Le attività possono essere eseguite nell'Administration Server e nei dispositivi.

Le seguenti attività vengono eseguite nell'Administration Server:

- Distribuzione automatica dei rapporti
- Download degli aggiornamenti nell'archivio di Administration Server
- Backup dei dati di Administration Server
- Manutenzione del database

I seguenti tipi di attività vengono eseguiti nei dispositivi:

- *Attività locali* - Attività eseguite in un dispositivo specifico

  Le attività locali possono essere modificate dall'amministratore utilizzando Kaspersky Security Center Web Console oppure dall'utente di un dispositivo remoto (ad esempio attraverso l'interfaccia dell'applicazione di protezione). Se un'attività locale viene modificata contemporaneamente dall'amministratore e dall'utente di un dispositivo gestito, hanno effetto le modifiche apportate dall'amministratore perché hanno una priorità più alta.

- *Attività di gruppo* - Attività eseguite su tutti i dispositivi di un gruppo specifico

  A meno che non sia diversamente specificato nelle proprietà dell'attività, un'attività di gruppo si applica anche a tutti i sottogruppi del gruppo selezionato. Un'attività di gruppo influisce anche (facoltativamente) sui dispositivi connessi agli Administration Server secondari e virtuali distribuiti nel gruppo o in uno dei relativi sottogruppi.

- *Attività globali* - Attività eseguite su un set di dispositivi, indipendentemente dalla loro appartenenza a un gruppo

Per ogni applicazione è possibile creare attività di gruppo, attività globali o attività locali.

È possibile apportare modifiche alle impostazioni delle attività, visualizzarne l'avanzamento, copiarle, esportarle, importarle ed eliminarle.

Le attività vengono avviate in un dispositivo solo se l'applicazione per cui l'attività è stata creata è in esecuzione.

I risultati delle attività sono salvati nel registro eventi Syslog e nel registro eventi di Kaspersky Security Center Linux, sia in modo centralizzato in Administration Server che localmente in ogni dispositivo.

Non includere dati privati nelle impostazioni dell'attività. Ad esempio, non specificare la password dell'amministratore del dominio.

Regole di spostamento dei dispositivi

È consigliabile automatizzare l'allocazione dei dispositivi ai gruppi di amministrazione attraverso le *regole di spostamento dei dispositivi*. Una regola di spostamento dei dispositivi comprende tre elementi principali: nome, condizione di esecuzione (espressione logica con gli attributi del dispositivo) e gruppo di amministrazione di destinazione. Una regola sposta un dispositivo nel gruppo di amministrazione di destinazione se gli attributi del dispositivo soddisfano la condizione di esecuzione della regola.

Tutte le regole di spostamento dei dispositivi hanno priorità. L'Administration Server verifica gli attributi del dispositivo per determinare se soddisfano la condizione di esecuzione di ogni regola, in ordine di priorità crescente. Se gli attributi del dispositivo soddisfano la condizione di esecuzione di una regola, il dispositivo viene spostato nel gruppo di destinazione, quindi l'elaborazione della regola è completa per questo dispositivo. Se gli attributi del dispositivo soddisfano le condizioni di più regole, il dispositivo viene spostato nel gruppo di destinazione della regola con la priorità più alta (al livello più alto nell'elenco delle regole).

Le regole di spostamento dei dispositivi possono essere create implicitamente. Ad esempio, nelle proprietà di un pacchetto di installazione o di un'attività di installazione remota è possibile specificare il gruppo di amministrazione in cui deve essere spostato il dispositivo dopo l'installazione di Network Agent. Inoltre, le regole di spostamento dei dispositivi possono essere create esplicitamente dall'amministratore di Kaspersky Security Center Linux nella sezione **Risorse (dispositivi)** → **Regole di spostamento**.

Per impostazione predefinita, una regola di spostamento dei dispositivi viene utilizzata per l'allocazione iniziale dei dispositivi ai gruppi di amministrazione. La regola sposta i dispositivi dal gruppo dei dispositivi non assegnati una sola volta. Se in precedenza un dispositivo era stato spostato da questa regola, la regola non lo sposterà di nuovo, anche se si reinserisce manualmente il dispositivo nel gruppo dei dispositivi non assegnati. Questo è il modo consigliato per applicare le regole di spostamento.

È possibile spostare i dispositivi che sono già stati assegnati ad alcuni gruppi di amministrazione. A tale scopo, nelle proprietà di una regola deselezionare la casella di controllo **Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione**.

L'applicazione delle regole di spostamento a dispositivi che sono già stati assegnati ad alcuni gruppi di amministrazione aumenta considerevolmente il carico sull'Administration Server.

La casella di controllo **Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione** è bloccata nelle proprietà delle regole di spostamento create automaticamente. Tali regole vengono create quando si aggiunge l'attività *Installa applicazione in remoto* o si crea un pacchetto di installazione indipendente.

È possibile creare una regola di spostamento da applicare ripetutamente a un singolo dispositivo.

È consigliabile evitare di spostare ripetutamente un singolo dispositivo da un gruppo all'altro (ad esempio, per applicare uno speciale criterio al dispositivo, eseguire una speciale attività di gruppo o aggiornare il dispositivo attraverso un punto di distribuzione specifico).

Tali scenari non sono supportati, perché comportano un notevole aumento del carico su Administration Server e del traffico di rete. Questi scenari sono anche in conflitto con i principi operativi di Kaspersky Security Center Linux (in particolare nell'area di diritti di accesso, eventi e rapporti). Un'altra soluzione deve ad esempio essere trovata attraverso l'utilizzo di profili criterio, attività per selezioni dispositivi, l'assegnazione di Network Agent in base allo scenario standard.

Classificazione del software

Lo strumento principale per monitorare l'esecuzione delle applicazioni sono le *categorie Kaspersky* (di seguito denominate anche *categorie KL*). Le categorie KL consentono agli amministratori di Kaspersky Security Center Linux di semplificare il supporto della classificazione del software e ridurre al minimo il traffico verso i dispositivi gestiti.

È necessario creare categorie utente per le applicazioni che non possono essere classificate in alcuna delle categorie KL esistenti (ad esempio, per il software personalizzato). Le categorie utente vengono create in base al pacchetto di installazione di un'applicazione (MSI) o a una cartella con pacchetti di installazione.

Se è disponibile una raccolta di software di grandi dimensioni che non è stata classificata tramite le categorie KL, può essere utile creare una categoria aggiornata automaticamente. I checksum dei file eseguibili saranno aggiunti automaticamente a questa categoria a ogni modifica della cartella che contiene i pacchetti di distribuzione.

Backup e ripristino delle impostazioni di Administration Server

Il backup delle impostazioni di Administration Server e del relativo database viene eseguito tramite l'attività di backup e l'utilità klbackup. Una copia di backup include tutte le impostazioni e gli oggetti principali relativi ad Administration Server, come certificati, chiavi primarie per il criptaggio delle unità nei dispositivi gestiti, chiavi per varie licenze, struttura dei gruppi di amministrazione con tutti i relativi contenuti, attività, criteri e così via. Con una copia di backup è possibile ripristinare il funzionamento di un Administration Server il prima possibile, un'operazione che richiede da una decina di minuti a un paio d'ore.

Se non è disponibile una copia di backup, un errore può comportare la perdita dei certificati e di tutte le impostazioni di Administration Server. In tal caso, sarà necessario riconfigurare completamente Kaspersky Security Center Linux ed eseguire di nuovo la distribuzione iniziale di Network Agent nella rete dell'organizzazione. Andranno inoltre perse tutte le chiavi primarie per il criptaggio delle unità nei dispositivi gestiti, con il rischio di una perdita irrevocabile dei dati criptati nei dispositivi con Kaspersky Endpoint Security. Pertanto, non dimenticare di eseguire periodicamente backup di Administration Server utilizzando l'attività di backup standard.

L'Avvio rapido guidato crea l'attività di backup per le impostazioni di Administration Server e ne configura l'esecuzione quotidiana, alle 4:00. Le copie di backup vengono salvate per impostazione predefinita nella cartella /var/opt/kaspersky/KSC_Backups*.

Poiché una copia di backup contiene dati importanti, l'attività di backup e l'utilità klbackup forniscono funzionalità di protezione tramite password delle copie di backup. Per impostazione predefinita, l'attività di backup viene creata con una password vuota. È necessario impostare una password nelle proprietà dell'attività di backup. Il mancato rispetto di questo requisito causa una situazione in cui tutte le chiavi dei certificati di Administration Server, le chiavi per le licenze e le chiavi primarie per il criptaggio delle unità nei dispositivi gestiti restano non criptate.

In aggiunta al backup periodico, è anche necessario creare una copia di backup prima di ogni modifica significativa, inclusa l'installazione di upgrade e patch di Administration Server.

Il ripristino da una copia di backup viene eseguito con l'utilità klbackup in un'istanza funzionante di Administration Server che è stata appena installata e con la stessa versione (o una versione successiva) di quella per cui è stata creata la copia di backup.

L'istanza di Administration Server in cui deve essere eseguito il ripristino deve utilizzare un DBMS dello stesso tipo e di una versione analoga o successiva. La versione di Administration Server può essere la stessa (con una patch identica o successiva) o una versione successiva.

In questa sezione sono descritti gli scenari standard per il ripristino delle impostazioni e degli oggetti di Administration Server.

Un dispositivo con Administration Server è inutilizzabile

Se un dispositivo con Administration Server risulta inutilizzabile a causa di un errore, è consigliabile eseguire le seguenti operazioni:

- Al nuovo Administration Server deve essere assegnato lo stesso indirizzo: nome DNS, o indirizzo IP statico (a seconda dell'elemento impostato al momento della distribuzione dei Network Agent).
- Installare Administration Server utilizzando un DBMS dello stesso tipo e della stessa versione (o di una versione successiva). È possibile installare la stessa versione del server (con una patch identica o successiva) o una versione successiva. Dopo installazione, non eseguire la configurazione iniziale tramite la procedura guidata.
- Eseguire l'utilità klbackup ed eseguire il ripristino.

Le impostazioni di Administration Server o il database sono danneggiati

Se Administration Server risulta inutilizzabile perché le impostazioni o il database sono danneggiati (ad esempio, in seguito a una sovralimentazione), è consigliabile utilizzare il seguente scenario di ripristino:

1. Eseguire la scansione del file system nel dispositivo danneggiato.
2. Disinstallare la versione inutilizzabile di Administration Server.
3. Reinstallare Administration Server utilizzando un DBMS dello stesso tipo e della stessa versione (o di una versione successiva). È possibile installare la stessa versione del server (con una patch identica o successiva) o una versione successiva. Dopo installazione, non eseguire la configurazione iniziale tramite la procedura guidata.
4. Eseguire l'utilità klbackup ed eseguire il ripristino.

Non è consentito ripristinare Administration Server in un modo diverso dall'utilizzo dell'utilità klbackup.

Qualsiasi tentativo di ripristinare Administration Server tramite software di terze parti causerà inevitabilmente la mancata sincronizzazione dei dati nei nodi dell'applicazione Kaspersky Security Center Linux distribuita e, di conseguenza, impedirà il corretto funzionamento dell'applicazione.

Informazioni sui profili di connessione per gli utenti fuori sede

Gli utenti fuori sede con computer portatili (di seguito denominati anche "dispositivi") possono aver bisogno di modificare il metodo di connessione a un Administration Server o passare da un Administration Server all'altro a seconda della posizione corrente del dispositivo nella rete aziendale.

I profili di connessione sono supportati solo per i dispositivi che eseguono Windows e macOS.

Utilizzo di differenti indirizzi di un singolo Administration Server

I dispositivi con Network Agent installato possono connettersi all'Administration Server dalla rete Intranet dell'organizzazione o da Internet. Questa situazione può richiedere l'utilizzo da parte di Network Agent di differenti indirizzi per la connessione ad Administration Server: l'indirizzo esterno dell'Administration Server per la connessione Internet e l'indirizzo interno dell'Administration Server per la connessione dalla rete interna.

A tale scopo, è necessario aggiungere un profilo (per la connessione ad Administration Server da Internet) al criterio di Network Agent. Aggiungere il profilo nelle proprietà del criterio (sezione **Connettività**, sottosezione **Profili connessione**). Nella finestra di creazione del profilo è necessario disabilitare l'opzione **Usa per ricevere solo aggiornamenti** e selezionare l'opzione **Sincronizza le impostazioni di connessione con le impostazioni di Administration Server specificate nel profilo**. Se si utilizza un gateway di connessione per accedere ad Administration Server (ad esempio, in una configurazione di Kaspersky Security Center Linux come quella descritta in Accesso a Internet: Network Agent come gateway nella rete perimetrale), è necessario specificare l'indirizzo del gateway di connessione nel campo corrispondente del profilo di connessione.

Passaggio da un Administration Server all'altro a seconda della rete corrente

Se l'organizzazione ha più sedi con diversi Administration Server e alcuni dispositivi con Network Agent installato si spostano tra di esse, è necessario che Network Agent si connetta all'Administration Server della rete locale nella sede in cui si trova attualmente il dispositivo.

In questo caso, è necessario creare un profilo per la connessione ad Administration Server nelle proprietà del criterio di Network Agent per ciascuna delle sedi, tranne che per la sede principale in cui si trova l'Administration Server principale originale. È necessario specificare gli indirizzi di Administration Server nei profili di connessione e abilitare o disabilitare l'opzione **Usa per ricevere solo aggiornamenti**:

- Selezionare l'opzione se è necessario sincronizzare Network Agent con l'Administration Server principale e utilizzare il server locale solo per scaricare gli aggiornamenti.
- Disabilitare questa opzione se è necessario che Network Agent sia completamente gestito dall'Administration Server locale.

Sarà quindi necessario impostare le condizioni per il passaggio ai nuovi profili creati: almeno una condizione per ciascuna delle sedi, tranne che per la sede principale. Lo scopo di ogni condizione consiste nel rilevamento degli elementi che sono specifici per l'ambiente di rete di una sede. Se una condizione è vera, il profilo corrispondente viene attivato. Se nessuna delle condizioni è vera, Network Agent passa all'Administration Server principale.

Accesso remoto ai dispositivi gestiti

In questa sezione vengono fornite informazioni sull'accesso remoto ai dispositivi gestiti.

Utilizzo dell'opzione "Non eseguire la disconnessione da Administration Server" per garantire connettività continua tra un dispositivo gestito e Administration Server

Se non si utilizzano server push, Kaspersky Security Center Linux non garantisce una connettività continua tra i dispositivi gestiti e Administration Server. I Network Agent nei dispositivi gestiti stabiliscono periodicamente connessioni ed eseguono la sincronizzazione con l'Administration Server. L'intervallo tra queste sessioni di sincronizzazione è definito in un criterio di Network Agent. Se è necessaria una sincronizzazione preventiva, Administration Server (o un punto di distribuzione, se in uso) invia un pacchetto di rete firmato tramite una rete IPv4 o IPv6 alla porta UDP di Network Agent. Il numero di porta predefinito è 15000. Se non è possibile stabilire la connessione tramite UDP tra Administration Server e un dispositivo gestito, la sincronizzazione verrà eseguita alla successiva connessione periodica di Network Agent ad Administration Server entro l'intervallo di sincronizzazione.

Alcune operazioni non possono essere eseguite senza una connessione preventiva tra Network Agent e Administration Server, come l'esecuzione e l'arresto di attività locali, la ricezione di statistiche per un'applicazione gestita. Per risolvere il problema, se non si utilizzano server push è possibile utilizzare l'opzione **Non eseguire la disconnessione da Administration Server** per assicurarsi che vi sia connettività continua tra un dispositivo gestito e Administration Server.

Per garantire connettività continua tra un dispositivo gestito e Administration Server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Nell'elenco dei dispositivi gestiti fare clic sul collegamento con il nome del dispositivo richiesto.

3. Nella sezione **Generale** della finestra delle proprietà del dispositivo, abilitare l'opzione **Non eseguire la disconnessione da Administration Server**.

Viene stabilita la connettività continua tra il dispositivo gestito e Administration Server.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Informazioni sul controllo del tempo di connessione tra un dispositivo e Administration Server

Al momento dell'arresto di un dispositivo, Network Agent invia una notifica all'Administration Server di questo evento. In Kaspersky Security Center Web Console il dispositivo viene visualizzato come spento. Tuttavia, Network Agent non può notificare ad Administration Server tutti gli eventi di questo tipo. Administration Server, pertanto, analizza periodicamente l'attributo **Connesso ad Administration Server** (il valore di questo attributo è visualizzato in Kaspersky Security Center Web Console nella sezione **Generale** delle proprietà del dispositivo) per ogni dispositivo e lo confronta con l'intervallo di sincronizzazione nelle impostazioni correnti di Network Agent. Se un dispositivo non risponde per più di tre intervalli di sincronizzazione consecutivi, il dispositivo è contrassegnato come arrestato.

Informazioni sulla sincronizzazione forzata

Anche se Kaspersky Security Center sincronizza automaticamente lo stato, le impostazioni, le attività e i criteri per i dispositivi gestiti, in alcuni casi l'amministratore ha l'esigenza di sapere esattamente se la sincronizzazione è stata già eseguita per un determinato dispositivo.

La finestra delle proprietà di un dispositivo gestito contiene il pulsante **Forza sincronizzazione**. Quando Kaspersky Security Center Linux esegue il comando di sincronizzazione, Administration Server tenta di connettersi al dispositivo. Se questo tentativo va a buon fine viene eseguita la sincronizzazione forzata. In caso contrario, la sincronizzazione verrà forzata solo dopo la successiva connessione pianificata tra Network Agent e l'Administration Server.

Guida per il dimensionamento

Questa sezione fornisce informazioni sul dimensionamento di Kaspersky Security Center Linux.

Informazioni sulla guida

La Guida per il dimensionamento di Kaspersky Security Center Linux (denominata anche Kaspersky Security Center) è destinata ai professionisti che si occupano dell'installazione e dell'amministrazione di Kaspersky Security Center, nonché a quelli che forniscono assistenza tecnica alle organizzazioni che utilizzano Kaspersky Security Center.

Tutti i suggerimenti e i calcoli vengono forniti per le reti in cui Kaspersky Security Center gestisce la protezione dei dispositivi in cui è installato il software Kaspersky.

Per ottenere e mantenere prestazioni ottimali in diverse condizioni operative, è necessario tenere conto del numero di dispositivi in rete, della topologia della rete e del set di funzionalità di Kaspersky Security Center richiesto.

La presente Guida fornisce le seguenti informazioni:

- Limitazioni di Kaspersky Security Center
- Calcoli per i nodi chiave di Kaspersky Security Center (Administration Server e punti di distribuzione):
  - Requisiti hardware per Administration Server e punti di distribuzione
  - Calcolo del numero e gerarchia degli Administration Server
  - Calcolo del numero e configurazione dei punti di distribuzione
- Configurazione della registrazione degli eventi nel database in base al numero dei dispositivi in rete
- Best practice comuni per l'ottimizzazione delle prestazioni
- Configurazione di attività specifiche mirate alle prestazioni ottimali di Kaspersky Security Center
- Frequenza di traffico (carico di rete) tra Kaspersky Security Center Administration Server e ciascun dispositivo protetto

È consigliabile consultare questa guida nei seguenti casi:

- In caso di pianificazione delle risorse prima dell'installazione di Kaspersky Security Center
- In caso di pianificazione di cambiamenti significativi della portata della rete in cui viene distribuito Kaspersky Security Center
- In caso di passaggio dall'utilizzo di Kaspersky Security Center all'interno di un segmento di rete limitato (un ambiente di test) alla distribuzione su vasta scala di Kaspersky Security Center nella rete aziendale
- In caso di modifiche al set di funzionalità di Kaspersky Security Center utilizzate

Calcoli per gli Administration Server

In questa sezione vengono specificati i requisiti software e hardware per i dispositivi utilizzati come Administration Server. Vengono inoltre forniti suggerimenti per il calcolo del numero e della gerarchia di Administration Server in base alla configurazione della rete dell'organizzazione.

Calcolo delle risorse hardware per Administration Server

Questa sezione contiene i calcoli che forniscono istruzioni sulla pianificazione delle risorse hardware per Administration Server.

Requisiti hardware per il DBMS e l'Administration Server

Nelle seguenti tabelle sono riportati i requisiti hardware minimi consigliati per un DBMS e un Administration Server ottenuti durante i test. Per un elenco completo di sistemi operativi e DBMS supportati fare riferimento all'elenco dei requisiti hardware e software.

La rete comprende 50.000 dispositivi

Configurazione del dispositivo in cui è installato Administration Server

Hardware	Valore
CPU	8 core (12 core consigliati), 2500 MHz
RAM	16 GB
Spazio su disco	300 GB, 150 IOPS o superiore

Configurazione del dispositivo in cui è installato PostgreSQL DBMS

Hardware	Valore
CPU	16 core, 2500 MHz
RAM	32 GB
Spazio su disco	300 GB, 150 IOPS o superiore

Configurazione del dispositivo in cui sono installati sia Administration Server e che PostgreSQL DBMS

Hardware	Valore
CPU	24 core (28 core consigliati), 2500 MHz
RAM	48 GB
Spazio su disco	600 GB, 300 IOPS o superiore

La rete comprende 30.000 dispositivi

Configurazione del dispositivo in cui è installato Administration Server

Hardware	Valore
CPU	6 core (8 core consigliati), 2500 MHz

RAM	12 GB
Spazio su disco	200 GB, 150 IOPS o superiore

Configurazione del dispositivo in cui è installato PostgreSQL DBMS

Hardware	Valore
CPU	12 core, 2500 MHz
RAM	24 GB
Spazio su disco	250 GB, 150 IOPS o superiore

Configurazione del dispositivo in cui sono installati sia Administration Server e che PostgreSQL DBMS

Hardware	Valore
CPU	18 core (6 core consigliati), 2500 MHz
RAM	36 GB
Spazio su disco	450 GB, 300 IOPS o superiore

La rete comprende 10.000 dispositivi

Configurazione del dispositivo in cui è installato Administration Server

Hardware	Valore
CPU	4 core (6 core consigliati), 2500 MHz
RAM	8 GB
Spazio su disco	100 GB, 150 IOPS o superiore

Configurazione del dispositivo in cui è installato PostgreSQL DBMS

Hardware	Valore
CPU	8 core, 2500 MHz
RAM	18 GB
Spazio su disco	200 GB, 150 IOPS o superiore

Configurazione del dispositivo in cui sono installati sia Administration Server e che PostgreSQL DBMS

Hardware	Valore
CPU	12 core (14 core consigliati), 2500 MHz
RAM	26 GB
Spazio su disco	300 GB, 300 IOPS o superiore

I test sono stati eseguiti con le seguenti impostazioni:

- L'assegnazione automatica dei punti di distribuzione è abilitata in Administration Server oppure i punti di distribuzione vengono assegnati manualmente in base alle tabella consigliata.
- Il DBMS PostgreSQL non include estensioni diverse da plpgsql.

Nel dispositivo in cui è installato il DBMS, il database utilizza circa 100 GB di spazio su disco e il registro delle transazioni utilizza circa 200 GB di spazio su disco.

Calcolo dello spazio del database

La quantità approssimativa di spazio che deve essere riservata nel database può essere calcolata utilizzando la seguente formula:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

dove:

- C è il numero dei dispositivi.
- E è il numero di eventi da memorizzare.
- A è il numero totale degli oggetti di Active Directory:
  - Account dispositivo
  - Account utente
  - Account dei gruppi di protezione
  - Unità organizzative di Active Directory

  Se la scansione di Active Directory è disabilitata, A è considerato uguale a zero.
- N è il numero medio di file eseguibili di cui è stato eseguito l'inventario in un dispositivo endpoint.
- F è il numero di dispositivi endpoint nei quali è stato eseguito l'inventario dei file eseguibili.

Se (nelle impostazioni dei criteri di Kaspersky Endpoint Security) si intende abilitare la notifica di Administration Server nelle applicazioni eseguite, è necessaria una quantità aggiuntiva di (0,03 * C) gigabyte per archiviare nel database le informazioni sulle applicazioni eseguite.

Durante l'esecuzione, nel database è sempre presente una determinata *quantità di spazio non allocato*. Pertanto, la dimensione effettiva del file di database risulta spesso essere circa il doppio della quantità di spazio occupato nel database.

Non è consigliabile limitare esplicitamente la dimensione del registro delle transazioni. È consigliabile mantenere il valore predefinito del parametro MAXSIZE.

Calcolo dello spazio su disco

Lo spazio su disco di Administration Server richiesto per la cartella var/opt/kaspersky/klnagent_srv/ può essere stimato approssimativamente utilizzando la formula:

(724 * C + 0,15 * E + 0,17 * A) KB

dove:

- C è il numero dei dispositivi.
- E è il numero di eventi da memorizzare.
- A è il numero totale degli oggetti di Active Directory:
  - Account dispositivo

- Account utente
- Account dei gruppi di protezione
- Unità organizzative di Active Directory

Se la scansione di Active Directory è disabilitata, A è considerato uguale a zero.

Calcolo del numero e configurazione degli Administration Server

Per ridurre il carico sull'Administration Server primario, è possibile assegnare un Administration Server separato a ciascun gruppo di amministrazione. Il numero di Administration Server secondari non può essere superiore a 500 per un singolo Administration Server primario.

È consigliabile creare la configurazione degli Administration Server in base alla configurazione della rete della propria organizzazione.

Suggerimenti per la connessione di macchine virtuali dinamiche a Kaspersky Security Center

Le macchine virtuali dinamiche (denominate anche VM dinamiche) consumano più risorse rispetto alle macchine virtuali statiche.

Per ulteriori informazioni sulle macchine virtuali dinamiche, vedere Supporto delle macchine virtuali dinamiche.

Quando viene connessa una nuova VM dinamica, Kaspersky Security Center Linux crea un record per questa VM dinamica in Kaspersky Security Center Web Console e sposta la VM dinamica nel gruppo di amministrazione. Successivamente, la VM dinamica viene aggiunta al database di Administration Server. Administration Server è completamente sincronizzato con Network Agent installato in questa VM dinamica.

Nella rete di un'organizzazione, Network Agent crea i seguenti elenchi di reti per ogni macchina virtuale dinamica:

- Hardware
- Software installato
- Vulnerabilità rilevate
- Eventi ed elenchi di file eseguibili del componente Controllo Applicazioni

Network Agent trasferisce questi elenchi di reti all'Administration Server. La dimensione degli elenchi di rete dipende dai componenti installati nella VM dinamica e può influire sulle prestazioni di Kaspersky Security Center Linux e il sistema di gestione database (DBMS). Si noti che il carico può crescere in modo non lineare.

Dopo che l'utente ha terminato di utilizzare la macchina virtuale dinamica e l'ha spenta, quest'ultima viene quindi rimossa dall'infrastruttura virtuale e le voci relative a questa macchina vengono rimosse dal database di Administration Server.

Tutte queste azioni consumano molte risorse del database di Kaspersky Security Center Linux e Administration Server e possono ridurre le prestazioni di Kaspersky Security Center Linux e DBMS. Si consiglia di connettere fino a 20.000 macchine virtuali dinamiche a Kaspersky Security Center Linux.

È possibile connettere più di 20.000 VM dinamiche a Kaspersky Security Center Linux se le VM dinamiche connesse eseguono operazioni standard (ad esempio, aggiornamenti del database) e consumano non più dell'80% della memoria e del 75-80% dei core disponibili.

La modifica delle impostazioni dei criteri, del software o del sistema operativo sulla VM dinamica può ridurre o aumentare il consumo di risorse. Il consumo dell'80-95% delle risorse è considerato ottimale.

Calcoli per punti di distribuzione e gateway di connessione

Questa sezione fornisce i requisiti hardware per i dispositivi utilizzati come punti di distribuzione insieme ai suggerimenti per il calcolo del numero di punti di distribuzione e di gateway di connessione in base alla configurazione della rete aziendale.

Requisiti per un punto di distribuzione

I requisiti hardware e software per i punti di distribuzione basati su Windows e Linux sono descritti in questo articolo.

Se in Administration Server è presente un'attività di installazione remota in sospeso, il dispositivo con il punto di distribuzione richiederà inoltre una quantità di spazio disponibile sul disco pari alle dimensioni totali dei pacchetti di installazione da installare.

Se in Administration Server sono presenti una o più istanze in sospeso delle attività di installazione degli aggiornamenti (patch) e di correzione delle vulnerabilità, il dispositivo con il punto di distribuzione richiederà ulteriore spazio disponibile sul disco, una quantità pari al doppio delle dimensioni totali di tutte le patch da installare.

Se si utilizza lo schema in cui i punti di distribuzione ricevono gli aggiornamenti dei database e dei moduli del software applicativo direttamente dai server di aggiornamento Kaspersky, i punti di distribuzione devono essere connessi a Internet.

Si sconsiglia di assegnare l'Administration Server come punto di distribuzione, poiché ciò aumenterà il carico sull'Administration Server.

Requisiti hardware per i punti di distribuzione basati su Windows

Requisiti hardware minimi per i punti di distribuzione basati su Windows

Numero di dispositivi client	CPU	RAM	RAM, con la gestione delle patch abilitata	Spazio su disco
10.000	4 core, 2500 MHz	8 GB	8 GB	120 GB
5000	4 core, 2500 MHz	6 GB	8 GB	120 GB
1000	2 core, 2500 MHz	4 GB	8 GB	120 GB

Requisiti hardware per i punti di distribuzione basati su Linux

Requisiti hardware minimi per i punti di distribuzione basati su Linux

Numero di dispositivi client	CPU	RAM	Spazio su disco

10.000	4 core, 2500 MHz	10 GB	120 GB
5000	4 core, 2500 MHz	8 GB	120 GB
1000	2 core, 2500 MHz	6 GB	120 GB

Calcolo del numero e configurazione dei punti di distribuzione

Più dispositivi client contiene una rete, maggiore è il numero dei punti di distribuzione richiesti. È consigliabile non disabilitare l'assegnazione automatica dei punti di distribuzione. Quando è abilitata l'assegnazione automatica dei punti di distribuzione, Administration Server assegna i punti di distribuzione se il numero dei dispositivi client è ampio e definisce la configurazione.

Utilizzo di punti di distribuzione assegnati in modo esclusivo

Se si prevede di utilizzare alcuni dispositivi specifici come punti di distribuzione (ovvero, server assegnati in modo esclusivo), è possibile scegliere di non utilizzare l'assegnazione automatica dei punti di distribuzione. In questo caso, verificare che i dispositivi a cui assegnare il ruolo di punti di distribuzione dispongano di un volume sufficiente di spazio libero su disco, che non vengano arrestati regolarmente e che la modalità di sospensione sia disabilitata.

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–100	1
Più di 100	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Utilizzo di dispositivi client standard (workstation) come punti di distribuzione

Se si prevede di utilizzare dispositivi client standard (ovvero, workstation) come punti di distribuzione, è consigliabile assegnare i punti di distribuzione come indicato nelle tabelle seguenti per evitare un carico eccessivo sui canali di comunicazione e su Administration Server:

Numero di workstation che operano come punti di distribuzione in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Numero di workstation che operano come punti di distribuzione in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–30	1
31–300	2

Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Se un punto di distribuzione viene arrestato (o non è disponibile per altri motivi), i dispositivi gestiti nel relativo ambito possono accedere ad Administration Server per gli aggiornamenti.

Calcolo del numero di gateway di connessione

Se si prevede di utilizzare un gateway di connessione, è consigliabile specificare un dispositivo specifico per questa funzione.

Un gateway di connessione può coprire un massimo di 10.000 dispositivi gestiti.

Registrazione delle informazioni sugli eventi per le attività e i criteri

Questa sezione contiene i calcoli associati all'archiviazione degli eventi nel database di Administration Server e offre suggerimenti su come ridurre al minimo il numero di eventi, riducendo quindi il carico su Administration Server.

Per impostazione predefinita, le proprietà di ogni attività e criterio consentono l'archiviazione di tutti gli eventi relativi all'esecuzione delle attività e all'applicazione dei criteri.

Tuttavia, se un'attività viene eseguita con una frequenza elevata (ad esempio più di una volta a settimana) e su un ampio numero di dispositivi (ad esempio più di 10.000), il numero di eventi può rivelarsi troppo ampio e gli eventi possono riempire eccessivamente il database. In questo caso è consigliabile selezionare una delle due opzioni nelle impostazioni dell'attività:

- **Salva eventi correlati all'avanzamento dell'attività**. In questo caso il database riceve solo le informazioni sull'avvio, sull'andamento e sul completamento dell'attività (completa, con avviso o con errore) da ciascun dispositivo in cui viene eseguita l'attività.

- **Salva solo i risultati dell'esecuzione dell'attività**. In questo caso il database riceve solo le informazioni sul completamento delle attività (completa, con avviso o con errore) da ciascun dispositivo in cui viene eseguita l'attività.

Se è stato definito un criterio per un ampio numero di dispositivi (ad esempio più di 10.000), il numero di eventi può anche rivelarsi troppo ampio e gli eventi possono riempire eccessivamente il database. In questo caso è consigliabile scegliere solo gli eventi più critici nelle impostazioni del criterio e abilitare la relativa registrazione. È consigliabile disabilitare la registrazione di tutti gli altri eventi.

In tal modo si riduce il numero di eventi nel database, si aumenta la velocità di esecuzione degli scenari associati all'analisi della tabella degli eventi nel database e si limita il rischio che gli eventi critici vengano sovrascritti da un ampio numero di eventi.

È anche possibile ridurre il periodo di archiviazione per gli eventi associati a un'attività o a un criterio. Il periodo predefinito è di 7 giorni per gli eventi correlati alle attività e di 30 giorni per gli eventi correlati ai criteri. Quando si modifica il periodo di archiviazione di un evento è opportuno prendere in considerazione le procedure operative in atto nell'organizzazione e la quantità di tempo che l'amministratore di sistema può dedicare all'analisi di ciascun evento.

È consigliabile modificare le impostazioni di archiviazione degli eventi in uno dei seguenti casi:

- Gli eventi riguardanti modifiche degli stati intermedi delle attività di gruppo e gli eventi correlati all'applicazione dei criteri occupano un'ampia quota del totale degli eventi nel database di Kaspersky Security Center Linux.

- Il registro del sistema operativo inizia a mostrare le voci relative alla rimozione automatica degli eventi quando viene superato il limite stabilito sul numero totale di eventi archiviati nel database.

Scegliere le opzioni di registrazione degli eventi partendo dal presupposto che il numero ottimale di eventi che derivano da un singolo dispositivo in un giorno non deve essere superiore a 20. È possibile aumentare leggermente questo limite, se necessario, ma solo se il numero di dispositivi nella rete è relativamente piccolo (inferiore a 10.000).

Best practice per un Administration Server che gestisce un numero elevato di dispositivi

Best practice per l'utilizzo del DBMS

Configurare l'attività di **Manutenzione di Administration Server** in modo che venga eseguita periodicamente, soprattutto se si utilizza un DBMS PostgreSQL.

Escludere la cartella DBMS dalla scansione IOC.

Best practice per criteri e profili

Ridurre il numero di criteri attivi per un componente (ad esempio, Kaspersky Endpoint Security for Windows). È possibile i criteri con i profili criterio.

Best practice per un Administration Server che gestisce un numero elevato di dispositivi

Ridurre il numero di attività eseguite contemporaneamente, in particolare l'installazione remota e la gestione delle patch.

Ridurre il numero e ottimizzare la pianificazione per le attività che funzionano con le selezioni dispositivi.

Nella sezione **Configurazione eventi** delle impostazioni dei criteri, ridurre al minimo il numero di tipi di evento salvati.

Best practice per l'archiviazione degli eventi

Ridurre la frequenza degli eventi di tipo singolo provenienti dal componente Controllo Applicazioni. Informazioni sul blocco degli eventi frequentiPer ulteriori dettagli, consultare l'argomento seguente: Informazioni sul blocco degli eventi frequenti.

Ridurre il periodo di archiviazione per gli eventi dei componenti (ad esempio, Kaspersky Endpoint Security for Windows) e gli eventi informativi sulle vulnerabilità corrette.

Abilitare l'opzione **Salva eventi correlati all'avanzamento dell'attività** nelle impostazioni dell'attività per le attività comuni, ad esempio le attività di aggiornamento. Registrazione delle informazioni sugli eventi per le attività e i criteriPer informazioni dettagliate, fare riferimento al seguente argomento: Registrazione delle informazioni sugli eventi per le attività e i criteri.

Ottimizzare le impostazioni dell'attività di inventario. Per ulteriori dettagli, fare riferimento al seguente argomento: Attività di inventario.

Considerazioni specifiche e impostazioni ottimali di determinate attività

Determinate attività sono soggette a considerazioni specifiche relative al numero di dispositivi di rete. Questa sezione offre suggerimenti sulla configurazione ottimale delle impostazioni per tali attività.

Device discovery, attività di backup dei dati, attività di manutenzione del database e attività di gruppo per aggiornare Kaspersky Endpoint Security fanno parte della funzionalità di base di Kaspersky Security Center Linux.

L'attività di inventario fa parte della funzionalità Vulnerability e patch management e non è disponibile se questa funzionalità non è attivata.

Frequenza della device discovery

Non è consigliabile aumentare la frequenza predefinita della device discovery poiché ciò può creare un carico eccessivo nei controller di dominio. È invece consigliabile pianificare il polling con la frequenza minima consentita dalle esigenze dell'organizzazione. Nella tabella di seguito vengono forniti i suggerimenti per il calcolo della pianificazione ottimale.

Pianificazione della device discovery

Numero di dispositivi nella rete	Frequenza consigliata per la device discovery
Minore di 10.000	Frequenza predefinita o inferiore
10.000 o superiore	Una volta al giorno o inferiore

Attività di backup dei dati di Administration Server e attività di manutenzione dei database

Administration Server smette di funzionare quando sono in esecuzione le seguenti attività:

- Backup dei dati di Administration Server
- Manutenzione di Administration Server

Quando queste attività sono in esecuzione, il database non può ricevere alcun dato.

Potrebbe essere necessario ripianificare queste attività in modo che non vengano eseguite contemporaneamente ad altre attività di Administration Server.

Attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security

Se Administration Server opera come sorgente degli aggiornamenti, l'opzione di pianificazione consigliata per le attività di aggiornamento di gruppo di Kaspersky Endpoint Security 10 e versioni successive è **Quando vengono scaricati nuovi aggiornamenti nell'archivio** con la casella di controllo **Usa automaticamente il ritardo casuale per l'avvio delle attività** selezionata.

Se si crea un'attività locale di download degli aggiornamenti dai server Kaspersky nell'archivio in ogni punto di distribuzione, la pianificazione periodica è consigliata per l'attività di aggiornamento di gruppo di Kaspersky Endpoint Security. In questo caso il valore del periodo con impostazione casuale deve essere di un'ora.

Attività di inventario

È possibile ridurre il carico sul database mentre si ottengono informazioni sui file eseguibili. A tale scopo, si consiglia di eseguire un'attività di inventario per Kaspersky Endpoint Security sui dispositivi di riferimento in cui è installato un set standard di software.

Il numero di file eseguibili ricevuti da Administration Server da un singolo dispositivo non può essere superiore a 150.000. Quando Kaspersky Security Center Linux raggiunge questo limite, non può ricevere nuovi file.

In genere, il numero di file in un dispositivo client comune non può essere superiore a 60.000. Il numero di file eseguibili in un file server può essere maggiore e può addirittura superare la soglia di 150.000.

Dettagli del carico di rete trasmesso fra Administration Server e dispositivi protetti

Questa sezione fornisce i risultati delle misurazioni di prova del traffico di rete con una descrizione delle condizioni di esecuzione delle misurazioni. È possibile fare riferimento a queste informazioni quando si pianifica l'infrastruttura di rete e la capacità di throughput dei canali di rete all'interno dell'organizzazione (o tra Administration Server e un'altra organizzazione con i dispositivi da proteggere). Conoscendo la capacità di throughput della rete, è inoltre possibile stimare approssimativamente il tempo richiesto dalle diverse operazioni di trasmissione dei dati.

Consumo del traffico in diversi scenari

La tabella di seguito consente di visualizzare i risultati dei test di misurazione condotti sul traffico tra Administration Server e un dispositivo gestito in scenari diversi.

Per impostazione predefinita, i dispositivi vengono sincronizzati con Administration Server ogni 15 minuti o con un intervallo più lungo. Tuttavia, se si modificano le impostazioni di un criterio o di un'attività in Administration Server, si verifica una sincronizzazione anticipata nei dispositivi a cui è applicabile il criterio (o l'attività), pertanto le nuove impostazioni vengono trasmesse ai dispositivi.

Frequenza di traffico tra Administration Server e un dispositivo gestito

Scenario	Traffico da Administration Server a ciascun dispositivo gestito	Traffico da ciascun dispositivo gestito ad Administration Server
Installazione di Kaspersky Endpoint Security for Linux con database aggiornati	390 MB	3,3 MB
Installazione di Network Agent	75 MB	397 KB
Installazione simultanea di Network Agent e Kaspersky Endpoint Security for Linux	459 MB	3.6 MB
Aggiornamento iniziale dei database anti-virus senza aggiornare i database nel pacchetto (se la partecipazione a Kaspersky Security Network è disabilitata)	113 MB	1,8 MB
Aggiornamento giornaliero dei database anti-virus (se la partecipazione a	22 MB	373 MB

Kaspersky Security Network è abilitata)		
Sincronizzazione iniziale prima dell'aggiornamento dei database in un dispositivo (trasferimento di criteri e attività)	382 KB	446 KB
Sincronizzazione iniziale dopo l'aggiornamento dei database in un dispositivo	20 KB	157 KB
Sincronizzazione senza modifiche in Administration Server (in base a una pianificazione)	18 KB	23 KB
Sincronizzazione quando una singola impostazione in un criterio di gruppo viene modificata (non appena l'impostazione viene modificata)	19 KB	20 KB
Sincronizzazione quando una singola impostazione in un'attività di gruppo viene modificata (non appena l'impostazione viene modificata)	14 KB	11 KB
Sincronizzazione forzata	110 KB	109 KB
Evento **Virus rilevato** (1 virus)	44 KB	50 KB
Evento **Virus rilevato** (10 virus)	58 KB	77 KB
Traffico occasionale dopo l'abilitazione dell'elenco Registro delle applicazioni	fino a 10 KB	fino a 12 KB
Traffico giornaliero quando è abilitato l'elenco Registro delle applicazioni	fino a 840 KB	fino a 1 MB

Utilizzo del traffico medio nell'arco di 24 ore

L'utilizzo medio del traffico tra Administration Server e un dispositivo gestito nell'arco di 24 ore è il seguente:

- Il traffico da Administration Server al dispositivo gestito è di 840 KB.
- Il traffico dal dispositivo gestito ad Administration Server è di 1 MB.

Il traffico è stato calcolato nell'ambito delle seguenti condizioni:

- Nel dispositivo gestito erano installati Network Agent e Kaspersky Endpoint Security for Linux.
- Al dispositivo non era assegnato un punto di distribuzione.
- Vulnerability e patch management non era abilitata.
- La frequenza di sincronizzazione con Administration Server era di 15 minuti.

Contatta Assistenza tecnica

Questa sezione descrive i modi e le condizioni per ottenere assistenza tecnica.

Come ottenere assistenza tecnica

Se non è possibile trovare una soluzione per il proprio problema nella documentazione di Kaspersky Security Center Linux o in una delle fonti di informazioni su Kaspersky Security Center Linux, contattare il Servizio di assistenza tecnica di Kaspersky. Gli specialisti del Servizio di assistenza tecnica risponderanno a tutte le domande relative all'installazione e all'utilizzo di Kaspersky Security Center Linux.

Kaspersky garantisce il supporto di Kaspersky Security Center Linux durante il ciclo di vita (vedere la pagina del ciclo di vita di supporto dell'applicazione). Prima di contattare il Servizio di assistenza tecnica, consultare le regole dell'assistenza.

È possibile contattare il Servizio di assistenza tecnica in uno dei seguenti modi:

- Visitando il sito Web del Servizio di assistenza tecnica
- Inviando una richiesta al Servizio di assistenza tecnica dal portale Kaspersky CompanyAccount

Assistenza tecnica tramite Kaspersky CompanyAccount

Kaspersky CompanyAccount è un portale per le aziende che utilizzano le applicazioni Kaspersky. Il portale Kaspersky CompanyAccount è progettato per facilitare l'interazione tra gli utenti e gli esperti di Kaspersky tramite richieste online. È possibile utilizzare Kaspersky CompanyAccount per tenere traccia dello stato delle proprie richieste online e visualizzarne la cronologia.

È possibile registrare tutti i dipendenti dell'organizzazione in un singolo account su Kaspersky CompanyAccount. Un singolo account consente di gestire in modo centralizzato le richieste online inviate a Kaspersky dai dipendenti registrati e di gestire i privilegi dei dipendenti tramite Kaspersky CompanyAccount.

Il portale Kaspersky CompanyAccount è disponibile nelle seguenti lingue:

- Inglese
- Spagnolo
- Italiano
- Tedesco
- Polacco
- Portoghese
- Russo
- Francese

- Giapponese

Per ulteriori informazioni su Kaspersky CompanyAccount, visitare il sito Web del Servizio di assistenza tecnica.

Recupero dei file di dump di Administration Server

I file di dump di Administration Server contengono tutte le informazioni sui processi di Administration Server in un determinato momento. I file di dump di Administration Server sono archiviati nella directory /var/lib/systemd/coredump. I file di dump vengono archiviati finché Kaspersky Security Center Linux è in uso e vengono eliminati definitivamente quando viene rimosso. I file di dump non vengono trasferiti automaticamente a Kaspersky.

Se Administration Server si arresta in modo anomalo, è possibile contattare l'Assistenza tecnica di Kaspersky; uno specialista dell'Assistenza tecnica potrebbe richiedere di inviare file di dump di Administration Server per ulteriori analisi a Kaspersky.

I file di dump possono contenere dati personali. Si consiglia di proteggere le informazioni dall'accesso non autorizzato prima di inviarle a Kaspersky.

Fonti di informazioni sull'applicazione

Pagina di Kaspersky Security Center Linux nel sito Web di Kaspersky

Nella pagina di Kaspersky Security Center Linux nel sito Web di Kaspersky, sono disponibili informazioni generali sull'applicazione e le relative funzionalità e caratteristiche.

Pagina di Kaspersky Security Center Linux nella Knowledge Base

La *Knowledge Base* è una sezione del sito Web del Servizio di assistenza tecnica di Kaspersky.

Nella pagina di Kaspersky Security Center Linux nella Knowledge Base, è possibile leggere articoli che forniscono informazioni utili, raccomandazioni e risposte alle domande frequenti su come acquistare, installare e utilizzare l'applicazione.

Gli articoli nella Knowledge Base possono fornire risposte a domande relative sia a Kaspersky Security Center Linux che ad altre applicazioni Kaspersky. Gli articoli nella Knowledge Base possono anche contenere notizie dal Servizio di assistenza tecnica.

Discutere delle applicazioni Kaspersky con la community

Se la domanda non richiede una risposta immediata, è possibile sottoporla agli esperti di Kaspersky e ad altri utenti nel nostro Forum.

Nel Forum, è possibile visualizzare gli argomenti di discussione, pubblicare i propri commenti e creare nuovi argomenti di discussione.

Per accedere alle risorse del sito Web, è necessaria una connessione a Internet.

Se non è possibile trovare una soluzione al problema, contattare il Servizio di assistenza tecnica.

Problemi noti

Kaspersky Security Center Linux presenta una serie di limitazioni non critiche per il funzionamento dell'applicazione:

- Quando si importa l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* o *Aggiorna verifica*, l'opzione **Selezionare i dispositivi a cui assegnare l'attività** è abilitata. Queste attività non possono essere assegnate a una selezione di dispositivi o a dispositivi specifici. Se si assegna l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* o *Aggiorna verifica* a dispositivi specifici, l'attività verrà importata in modo errato.

- Se la rete include un dominio Microsoft Active Directory che contiene diverse decine di migliaia di oggetti (dispositivi gestiti, gruppi di protezione e account utente) e le dimensioni della pagina di risposta (il parametro `MaxPageSize`) sono inferiori a 5.000, il polling del controller di dominio non è disponibile e le informazioni sugli oggetti del dominio non vengono ricevute. Quando si tenta di eseguire il polling del controller di dominio, si verifica l'errore *Limite di dimensioni superato*. L'aumento delle dimensioni della pagina di risposta può contribuire a correggere l'errore. È possibile utilizzare l'utilità Ntdsutil.exe per aumentare il valore del parametro `MaxPageSize` a `5000` o a `10000`, se necessario.

- Quando si abilita KPSN nelle proprietà di Administration Server e si utilizza la porta HTTPS 17111, la connessione con ds.kaspersky.com non viene interrotta.

- Kaspersky Endpoint Security for Windows non supporta il servizio Proxy KSN se l'opzione **Usa HTTPS** è abilitata nelle impostazioni del proxy KSN delle proprietà di Administration Server e l'indirizzo di Administration Server contiene caratteri non latini.

- Quando si passa a un server secondario dall'interfaccia di un Administration Server primario di Kaspersky Security Center Linux, non è possibile aprire la sezione **Aggiornamenti immediati** del menu principale.

- Quando si crea l'attività *Aggiungi chiave* per Kaspersky Endpoint Security 11.3 for Mac, la procedura guidata mostra una tabella delle chiavi di licenza che può contenere righe vuote.

- Il livello di protezione visualizzato nel criterio di Kaspersky Endpoint Security for Windows non corrisponde al livello di protezione nell'interfaccia di Kaspersky Endpoint Security for Windows.

- Quando si esegue l'attività *Disinstalla l'applicazione in remoto* per rimuovere un'applicazione Kaspersky da un dispositivo gestito, l'attività viene completata correttamente, ma l'applicazione non viene rimossa. Questo problema è valido per Kaspersky Endpoint Security for Linux, Kaspersky Embedded Systems Security for Linux e Kaspersky Industrial CyberSecurity for Linux Nodes.

- La finestra delle proprietà di Administration Server contiene le impostazioni per i dispositivi mobili, sebbene Kaspersky Security Center Linux non supporti la gestione dei dispositivi mobili.

- Se un'applicazione nella sezione **Registro delle applicazioni** è stata rilevata in un dispositivo Linux, le proprietà dell'applicazione non contengono informazioni sui file eseguibili correlati.

- Se si installa Network Agent in un dispositivo in cui viene eseguito il sistema operativo ALT Linux tramite un'attività di installazione remota e si esegue questa attività con un account con privilegi non root, l'attività non riesce. Eseguire l'attività di installazione remota con l'account root oppure creare e utilizzare un pacchetto di installazione indipendente di Network Agent per installare l'applicazione in locale.

- Nei rapporti con formato lettera, un'interruzione di pagina può tagliare orizzontalmente una riga di testo.

- Nella procedura guidata **Aggiungi Administration Server secondario**, se si specifica un account con la verifica in due passaggi abilitata per l'autenticazione sul futuro server secondario, la procedura guidata termina con un errore. Per risolvere questo problema, specificare un account per il quale la verifica in due passaggi è disabilitata o creare la gerarchia dal futuro server secondario.

- Se si apre Kaspersky Security Center Web Console in browser diversi e si scarica il file del certificato dell'Administration Server nella finestra delle proprietà dell'Administration Server, i file scaricati hanno nomi diversi.

- Un dispositivo gestito che dispone di più schede di rete invia all'Administration Server informazioni sull'indirizzo MAC della scheda di rete che non sono quelle utilizzate per la connessione all'Administration Server.

- In Astra Linux a 64 bit, il pacchetto klnagent-astra non può essere aggiornato con il pacchetto klnagent64_14: il pacchetto klnagent64-astra precedente verrà rimosso e verrà installato il nuovo pacchetto klnagent64 anziché l'aggiornamento, quindi verrà aggiunta la nuova icona del dispositivo con il pacchetto klnagent64_14. È possibile rimuovere l'icona precedente per questo dispositivo.

Glossario

Administration Console

Un componente di Kaspersky Security Center basato su Windows (denominato anche Administration Console basata su MMC). Questo componente offre un'interfaccia utente per i servizi di amministrazione di Administration Server e Network Agent. Administration Console è il corrispondente di Kaspersky Security Center Web Console.

Administration Server

Un componente di Kaspersky Security Center Linux che archivia in modo centralizzato le informazioni su tutte le applicazioni Kaspersky installate nella rete aziendale. È inoltre possibile utilizzarlo per la gestione di tali applicazioni.

Administration Server principale

Per Administration Server principale si intende l'Administration Server che è stato specificato durante l'installazione di Network Agent. L'Administration Server principale può essere utilizzato nelle impostazioni dei profili di connessione di Network Agent.

Administration Server virtuale

Componente di Kaspersky Security Center Linux progettato per la gestione del sistema di protezione della rete di un'organizzazione client.

Un Administration Server virtuale è un particolare tipo di Administration Server secondario e presenta le seguenti limitazioni rispetto a un Administration Server fisico:

- Un Administration Server virtuale può essere creato solo in un Administration Server primario.
- L'Administration Server virtuale utilizza il database dell'Administration Server primario durante il relativo funzionamento. Le attività di backup e ripristino dei dati, nonché le attività di scansione e download degli aggiornamenti, non sono supportate in un Administration Server virtuale.
- Un server virtuale non supporta la creazione di Administration Server secondari (inclusi server virtuali).

Agente di Autenticazione

Interfaccia che consente di completare l'autenticazione per l'accesso ai dischi rigidi criptati e il caricamento del sistema operativo dopo il criptaggio del disco rigido avviabile.

Aggiorna

Procedura di sostituzione o aggiunta di nuovi file (database o moduli dell'applicazione) recuperati dai server degli aggiornamenti di Kaspersky.

Aggiornamento disponibile

Un set di aggiornamenti per i moduli dell'applicazione Kaspersky, inclusi gli aggiornamenti critici accumulati in un determinato periodo di tempo e modifiche all'architettura dell'applicazione.

Amministratore client

Membro dello staff di un'organizzazione client responsabile del monitoraggio dello stato della protezione anti-virus.

Amministratore del provider di servizi

Membro dello staff di un provider di servizi di protezione anti-virus. Questo amministratore esegue i processi di installazione e manutenzione per i sistemi di protezione anti-virus basati sui prodotti Kaspersky, oltre a fornire assistenza tecnica ai clienti.

Amministratore di Kaspersky Security Center Linux

La persona che gestisce le operazioni dell'applicazione tramite il sistema centralizzato di amministrazione remota Kaspersky Security Center Linux.

Applicazione incompatibile

Un'applicazione anti-virus di uno sviluppatore di terze parti o un'applicazione Kaspersky che non supporta la gestione tramite Kaspersky Security Center Linux.

Archivio eventi

Una parte del database di Administration Server dedicato all'archiviazione delle informazioni sugli eventi che si verificano in Kaspersky Security Center Linux.

Attività

Le funzioni eseguite dall'applicazione Kaspersky sono implementate come attività, ad esempio Protezione in tempo reale, Scansione completa del computer e Aggiornamento database.

Attività di gruppo

Un'attività definita per un gruppo di amministrazione ed eseguita in tutti i dispositivi client inclusi nel gruppo di amministrazione.

Attività locale

Attività definita e in esecuzione in un singolo computer client.

Attività per dispositivi specifici

Attività assegnata a un set di dispositivi client appartenenti a gruppi di amministrazione arbitrari ed eseguita su tali dispositivi.

Backup dei dati di Administration Server

Copia dei dati di Administration Server per il backup e il successivo ripristino eseguita tramite l'utilità di backup. L'utilità consente di salvare:

- Database di Administration Server (criteri, attività, impostazioni delle applicazioni, eventi salvati in Administration Server)
- Informazioni sulla configurazione della struttura dei gruppi di amministrazione e dei dispositivi client
- Archivio dei file di installazione per l'installazione remota delle applicazioni (contenuto delle cartelle: Pacchetti, Disinstallazione e Aggiornamenti)
- Certificato di Administration Server

Cartella di backup

Speciale cartella per la memorizzazione delle copie dei dati di Administration Server create tramite l'utilità di backup.

Certificato condiviso

Certificato che consente di identificare il dispositivo mobile dell'utente.

Certificato di Administration Server

Il certificato utilizzato da Administration Server per i seguenti scopi:

- Autenticazione di Administration Server durante la connessione a Kaspersky Security Center Web Console
- Interazione sicura tra Administration Server e Network Agent nei dispositivi gestiti
- Autenticazione degli Administration Server durante la connessione di un Administration Server primario a un Administration Server secondario

Il certificato viene creato automaticamente quando si installa Administration Server e quindi archiviato in Administration Server.

Chiave attiva

Chiave attualmente utilizzata dall'applicazione.

Chiave di licenza aggiuntiva (o di riserva)

Una chiave che convalida il diritto di utilizzo dell'applicazione, ma non è attualmente utilizzata.

Client di Administration Server (dispositivo client)

Dispositivo, server o workstation in cui è installato Network Agent e sono in esecuzione le applicazioni Kaspersky gestite.

Criterio

Un criterio determina le impostazioni di un'applicazione e gestisce la capacità di configurare tale applicazione nei computer all'interno di un gruppo di amministrazione. Per ogni applicazione è necessario creare un criterio individuale. È possibile creare più criteri per le applicazioni installate nei computer di ciascun gruppo di amministrazione, ma a ogni applicazione è possibile applicare un solo criterio per volta all'interno di un gruppo di amministrazione.

Database anti-virus

Database che contengono informazioni sulle minacce per la protezione del computer note a Kaspersky al momento del rilascio dei database anti-virus. Le voci contenute nei database anti-virus consentono il rilevamento del codice dannoso negli oggetti esaminati. I database anti-virus sono creati dagli specialisti di Kaspersky e vengono aggiornati ogni ora.

Diritti di amministratore

Livello di diritti e privilegi dell'utente necessari per l'amministrazione di oggetti Exchange all'interno di un'organizzazione Exchange.

Dispositivi gestiti

Dispositivi della rete aziendale inclusi in un gruppo di amministrazione.

Dominio di trasmissione

Un'area logica di una rete in cui tutti i nodi possono scambiare dati utilizzando un canale di trasmissione al livello OSI (Open Systems Interconnection Basic Reference Model).

File chiave

Un file nel formato xxxxxxxx.key che consente l'utilizzo di un'applicazione Kaspersky in base ai termini della licenza commerciale o di prova.

Gateway di connessione

Un *gateway di connessione* è un Network Agent che funziona in modalità speciale. Un gateway di connessione accetta le connessioni da altri Network Agent e le trasmette ad Administration Server tramite la propria connessione con il server. A differenza di un normale Network Agent, un gateway di connessione attende le connessioni da Administration Server anziché stabilire connessioni ad Administration Server.

Gestione centralizzata delle applicazioni

Gestione remota delle applicazioni tramite i servizi di amministrazione forniti da Kaspersky Security Center.

Gestione diretta delle applicazioni

Gestione applicazioni tramite un'interfaccia locale.

Gruppo di amministrazione

Un set di dispositivi raggruppati in base alla funzione e alle applicazioni Kaspersky installate. I dispositivi sono raggruppati come una singola entità per semplificare la gestione. Un gruppo può includere altri gruppi. È possibile creare criteri di gruppo e attività di gruppo per ogni applicazione installata nel gruppo.

Gruppo di ruoli

Gruppo di utenti di dispositivi mobili Exchange ActiveSync a cui sono stati concessi diritti di amministratore identici.

HTTPS

Protocollo sicuro per il trasferimento dei dati tramite criptaggio tra un browser e un server Web. HTTPS viene utilizzato per ottenere l'accesso a informazioni con restrizioni, quali dati aziendali o finanziari.

Impostazioni attività

Impostazioni dell'applicazione specifiche per ogni tipo di attività.

Impostazioni del programma

Impostazioni dell'applicazione comuni a tutti i tipi di attività e che determinano il funzionamento generale dell'applicazione, ad esempio: impostazioni relative alle prestazioni dell'applicazione, impostazioni dei rapporti e impostazioni di backup.

Installazione locale

Installazione di un'applicazione di protezione in un dispositivo di una rete aziendale che presuppone l'avvio manuale dell'installazione dal pacchetto di distribuzione dell'applicazione di protezione o l'avvio manuale di un pacchetto di installazione pubblicato che è stato scaricato preventivamente nel dispositivo.

Installazione manuale

Installazione di un'applicazione di protezione in un dispositivo della rete aziendale dal pacchetto di distribuzione. L'installazione manuale richiede il coinvolgimento di un amministratore o di un altro specialista IT. In genere l'installazione manuale viene eseguita se l'installazione remota è stata completata con un errore.

Installazione remota

Installazione delle applicazioni Kaspersky utilizzando i servizi offerti da Kaspersky Security Center Linux.

JavaScript

Linguaggio di programmazione che estende le prestazioni delle pagine Web. Le pagine Web create tramite JavaScript possono eseguire funzioni (ad esempio, modificare la visualizzazione di elementi di interfaccia o aprire ulteriori finestre) senza aggiornare la pagina Web con nuovi dati dal server Web. Per visualizzare le pagine create utilizzando JavaScript, abilitare il supporto per JavaScript nella configurazione del browser.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network è una soluzione che consente agli utenti dei dispositivi in cui sono installate le applicazioni Kaspersky di accedere ai database di reputazione di Kaspersky Security Network e ad altri dati statistici senza inviare dati dai propri dispositivi a Kaspersky Security Network. Kaspersky Private Security Network è progettato per i clienti aziendali che non sono in grado di partecipare al programma Kaspersky Security Network per uno dei seguenti motivi:

- I dispositivi non sono connessi a Internet.

- La trasmissione dei dati all'esterno del paese o della rete LAN aziendale è vietata dalla legge o dai criteri di protezione aziendali.

Kaspersky Security Center Linux Web Server

Componente di Kaspersky Security Center Linux installato insieme ad Administration Server. Il server Web è progettato per la trasmissione tramite una rete di pacchetti di installazione indipendenti, profili MDM iOS e file da una cartella condivisa.

Kaspersky Security Center System Health Validator (SHV)

Un componente Kaspersky Security Center Linux utilizzato per la verifica della possibilità di utilizzare il sistema operativo in caso siano in esecuzione contemporaneamente Kaspersky Security Center Linux e Microsoft NAP.

Lightweight Nagent (LWNGT)

Un protocollo per l'interazione con Kaspersky Endpoint Security sui dispositivi mobili. Il protocollo LWNGT (chiamato anche protocollo Mobile) funziona come Network Agent senza dover effettivamente installare il programma di installazione di Network Agent sui dispositivi mobili.

Livello di criticità di un evento

Una proprietà di un evento verificatosi durante l'esecuzione di un'applicazione Kaspersky. Esistono i seguenti livelli di criticità:

- Evento critico
- Errore funzionale
- Avviso
- Informazioni

Eventi dello stesso tipo possono avere diversi livelli di criticità, a seconda della situazione in cui si è verificato l'evento.

Negozio applicazioni

Componente di Kaspersky Security Center Linux. Il negozio applicazioni viene utilizzato per installare le applicazioni nei dispositivi Android di proprietà degli utenti. Il negozio applicazioni consente di pubblicare i file APK delle applicazioni e i collegamenti alle applicazioni in Google Play.

Network Agent

Un componente di Kaspersky Security Center Linux che consente l'interazione tra Administration Server e le applicazioni Kaspersky installate in un nodo di rete specifico (workstation o server). Questo componente è comune a tutte le applicazioni dell'azienda per Microsoft® Windows®. Esistono versioni distinte di Network Agent per le applicazioni Kaspersky sviluppate per i sistemi operativi Unix e macOS.

Network Location Awareness (NLA)

Servizio Windows che aiuta un sistema operativo a identificare la rete corrente. NLA rileva le modifiche alla rete e regola la configurazione di protezione del dispositivo.

Operatore di Kaspersky Security Center

Utente che monitora lo stato e l'esecuzione di un sistema di protezione gestito tramite Kaspersky Security Center.

Pacchetto di installazione

Un set di file creati per l'installazione remota di un'applicazione Kaspersky tramite il sistema di amministrazione remota Kaspersky Security Center. Il pacchetto di installazione contiene numerose impostazioni necessarie per installare l'applicazione e renderla operativa subito dopo l'installazione. Le impostazioni corrispondono alle impostazioni predefinite dell'applicazione. Il pacchetto di installazione viene creato utilizzando i file con le estensioni kpd e kud inclusi nel kit di distribuzione dell'applicazione.

Periodo licenza

Il periodo di tempo durante il quale l'utente ha accesso alle funzionalità dell'applicazione e dispone dei diritti necessari per utilizzare i servizi aggiuntivi. I servizi che possono essere utilizzati dipendono dal tipo di licenza.

Profilo

Un insieme di impostazioni dei dispositivi mobili Exchange che definisce il loro comportamento durante la connessione a un server Microsoft Exchange.

Profilo di configurazione

Criterio che contiene un insieme di impostazioni e limitazioni per un dispositivo mobile MDM iOS.

Profilo di provisioning

Insieme di impostazioni per l'esecuzione delle applicazioni nei dispositivi mobili iOS. Un profilo di provisioning contiene le informazioni sulla licenza ed è collegato a una specifica applicazione.

Proprietario dispositivo

Il proprietario dispositivo è un utente che l'amministratore può contattare quando si rende necessario eseguire determinate operazioni con un dispositivo client.

Protezione anti-virus della rete

Set di misure tecniche e organizzative che riducono il rischio di penetrazione di virus e spam nella rete di un'organizzazione, oltre a impedire attacchi di rete, phishing e altre minacce. La sicurezza di rete aumenta quando si utilizzano applicazioni e servizi di protezione e quando si applicano e si rispettano i criteri di protezione dei dati aziendali.

Provider di servizi di protezione anti-virus

Organizzazione che fornisce a un'organizzazione client servizi di protezione anti-virus basati sulle soluzioni Kaspersky.

Punto di distribuzione

Computer in cui è installato Network Agent e che viene utilizzato per la distribuzione di aggiornamenti, l'installazione remota di applicazioni, l'acquisizione di informazioni sui computer in un gruppo di amministrazione e/o la trasmissione in un dominio. I punti di distribuzione hanno l'obiettivo di ridurre il carico sull'Administration Server durante la distribuzione degli aggiornamenti e di ottimizzare il traffico di rete. I punti di distribuzione possono essere assegnati automaticamente dall'Administration Server o manualmente dall'amministratore. Il punto di distribuzione era precedentemente noto come Update Agent.

Rete perimetrale (DMZ)

La rete perimetrale è un segmento di una rete locale in cui sono contenuti i server che risponde alle richieste del Web globale. Per garantire la protezione della rete locale di un'organizzazione, l'accesso alla LAN dalla rete perimetrale è protetto tramite firewall.

Ripristino

Riposizionamento dell'oggetto originale dalle cartelle Quarantena o Backup nella cartella originale in cui era memorizzato prima di essere messo in quarantena, disinfettato o eliminato, oppure in una cartella definita dall'utente.

Ripristino dei dati di Administration Server

Ripristino dei dati di Administration Server dalle informazioni salvate in Backup tramite l'utilità di backup. L'utilità consente di ripristinare:

- Database di Administration Server (criteri, attività, impostazioni delle applicazioni, eventi salvati in Administration Server)
- Informazioni sulla configurazione della struttura dei gruppi di amministrazione e dei dispositivi client
- Archivio dei file di installazione per l'installazione remota delle applicazioni (contenuto delle cartelle: Pacchetti, Disinstallazione e Aggiornamenti)
- Certificato di Administration Server

Server degli aggiornamenti Kaspersky

I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.

SSL

Protocollo di criptaggio dei dati utilizzato per Internet e le reti locali. Secure Sockets Layer (SSL) viene utilizzato nelle applicazioni Web per creare una connessione protetta tra un client e un server.

Stato della protezione della rete

Stato della protezione corrente, che definisce la sicurezza dei dispositivi della rete aziendale. Lo stato della protezione della rete include fattori come le applicazioni di protezione installate, l'utilizzo delle chiavi di licenza e il numero e i tipi di minacce rilevate.

Stato protezione

Stato corrente della protezione, che riflette il livello di protezione del computer.

Utenti interni

Gli account degli utenti interni vengono utilizzati per operare con gli Administration Server virtuali. Kaspersky Security Center Linux concede agli utenti interni dell'applicazione diritti equivalenti a quelli degli utenti reali.

Gli account degli utenti interni vengono creati e utilizzati solo in Kaspersky Security Center Linux. Nessun dato relativo agli utenti interni viene trasferito al sistema operativo. Kaspersky Security Center Linux esegue l'autenticazione degli utenti interni.

Workstation dell'amministratore

Un dispositivo da cui si apre Kaspersky Security Center Web Console. Questo componente fornisce un'interfaccia di gestione per Kaspersky Security Center Linux.

La workstation dell'amministratore viene utilizzata per configurare e gestire la parte server di Kaspersky Security Center Linux. Utilizzando la workstation dell'amministratore, l'amministratore crea e gestisce un sistema centralizzato della protezione anti-virus per la rete LAN aziendale basato sulle applicazioni Kaspersky.

Informazioni sul codice di terze parti

Le informazioni sul codice di terze parti sono contenute nel file denominato legal_notices.txt, disponibile nella directory di installazione dell'applicazione.

Note relative ai marchi registrati

I marchi registrati e i marchi di servizi sono di proprietà dei rispettivi titolari.

Adobe, Acrobat, Flash, Shockwave e PostScript sono marchi o marchi registrati di Adobe negli Stati Uniti e/o in altri paesi.

AMD e AMD64 sono marchi o marchi registrati di Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace sono marchi registrati di Amazon.com, Inc. o delle relative consociate.

Apache è un marchio registrato o un marchio di 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 e Touch ID sono marchi di Apple Inc.

Arm è un marchio registrato di Arm Limited (o delle sue filiali) negli Stati Uniti e/o altrove.

La parola, il marchio e i logo Bluetooth sono di proprietà di Bluetooth SIG, Inc.

Ubuntu, LTS sono marchi registrati di Canonical Ltd.

Cisco, Cisco Jabber, Cisco Systems, IOS sono marchi o marchi registrati di Cisco Systems, Inc. e/o delle relative consociate negli Stati Uniti e in altri paesi.

Citrix, XenServer sono marchi registrati o marchi di Cloud Software Group, Inc. e/o delle sue consociate negli Stati Uniti e/o in altri paesi.

Corel è un marchio o un marchio registrato di Corel Corporation e/o delle relative filiali in Canada, negli Stati Uniti e/o in altri paesi.

Cloudflare, il logo Cloudflare e Cloudflare Workers sono marchi e/o marchi registrati di Cloudflare, Inc. negli Stati Uniti e in altre giurisdizioni.

Dropbox è un marchio di Dropbox, Inc.

Radmin è un marchio registrato di Famatech.

Firebird è un marchio registrato di Firebird Foundation.

Foxit è un marchio registrato di Foxit Corporation.

FreeBSD è un marchio registrato di The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Google Public DNS, Hangouts e YouTube sono marchi di Google LLC.

EulerOS, FusionCompute, FusionSphere sono marchi di Huawei Technologies Co., Ltd.

Intel, Core, Xeon sono marchi registrati di Intel Corporation o delle sue affiliate.

IBM, QRadar sono marchi di International Business Machines Corporation, registrati presso diverse giurisdizioni a livello mondiale.

Node.js è un marchio di Joyent, Inc.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e in altri paesi.

Logitech è un marchio o un marchio registrato di Logitech negli Stati Uniti e in altri paesi.

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 e Windows Azure sono marchi del gruppo di società Microsoft.

Mozilla, Firefox, Thunderbird sono marchi di Mozilla Foundation negli Stati Uniti e in altri paesi.

Novell è un marchio registrato di Novell Enterprises Inc. negli Stati Uniti e in altri paesi.

OpenSSL è un marchio di proprietà di OpenSSL Software Foundation.

Oracle, Java, JavaScript e TouchDown sono marchi registrati di Oracle e/o delle relative consociate.

Parallels, il logo Parallels e Coherence sono marchi o marchi registrati di Parallels International GmbH.

Chef è un marchio o un marchio registrato di Progress Software Corporation e/o di una delle relative consociate o filiali negli Stati Uniti e/o in altri paesi.

Puppet è un marchio o un marchio registrato di Puppet, Inc.

Python è un marchio o un marchio registrato di Python Software Foundation.

Red Hat, Fedora e Red Hat Enterprise Linux sono marchi o marchi registrati di Red Hat, Inc. o delle relative consociate negli Stati Uniti e in altri paesi.

Ansible è un marchio registrato di Red Hat. Inc. negli Stati Uniti e in altri paesi.

CentOS è un marchio o un marchio registrato di Red Hat, Inc. o delle relative consociate negli Stati Uniti e in altri paesi.

Il marchio BlackBerry è di proprietà di Research In Motion Limited ed è registrato negli Stati Uniti e potrebbe essere registrato o in attesa di registrazione in altri paesi.

Debian è un marchio registrato di Software in the Public Interest, Inc.

Splunk, SPL sono marchi e marchi registrati di Splunk Inc. negli Stati Uniti e in altri paesi.

SUSE è un marchio registrato di SUSE LLC negli Stati Uniti e in altri paesi.

Symbian è un marchio registrato di proprietà di Symbian Foundation Ltd.

OpenAPI è un marchio di Linux Foundation.

UNIX è un marchio registrato negli Stati Uniti e in altri paesi, concesso in licenza in esclusiva tramite X/Open Company Limited.

Zabbix è un marchio registrato di Zabbix SIA.