Sommario

Guida di Kaspersky Security Center 14 Linux

Novità

Informazioni sulle novità della versione più recente dell'applicazione.

Requisiti hardware e software

Controllare i sistemi operativi e le versioni delle applicazioni supportati.

Installazione

Installare Administration Server e Kaspersky Security Center 14 Web Console.

Individuazione dei dispositivi nella rete

Individuare i dispositivi nuovi ed esistenti nella rete dell'organizzazione.

Applicazioni Kaspersky. Distribuzione centralizzata

Applicazioni Kaspersky. Licensing e attivazione

Attivare le applicazioni Kaspersky in pochi passaggi.

Configurazione della protezione di rete

Gestire la protezione dell'organizzazione.

Applicazioni Kaspersky. Aggiornamento dei database e dei moduli del software

Gestire l'affidabilità del sistema di protezione.

Monitoraggio e generazione di rapporti

Visualizzare l'infrastruttura, lo stato della protezione e le statistiche.

Regolazione di punti di distribuzione e/o gateway di

Distribuire applicazioni Kaspersky.

connessione

Configurare i punti di distribuzione.

Novità

Guida di Kaspersky Security Center 14 Linux

Kaspersky Security Center Linux 14 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 adesso possono 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 scarica dai server di aggiornamento Kaspersky solo gli aggiornamenti richiesti dalle applicazioni di sicurezza 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 *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.

Informazioni su Kaspersky Security Center Linux

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

Kaspersky Security Center Linux (denominato anche Kaspersky Security Center) è progettato per distribuire e gestire la protezione dei dispositivi Linux® utilizzando Administration Server basato su Linux per soddisfare i requisiti degli ambienti Linux puri.

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.
- 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.

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.

Requisiti hardware e software

Administration Server

Requisiti hardware insufficienti:

- 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: 4 GB.
- Spazio disponibile su disco: 10 GB.

Sono supportati i seguenti sistemi operativi:

- Debian GNU/Linux 11.x (Bullseye) 32 bit/64 bit
- Debian GNU/Linux 10.x (Buster) 32-bit/64-bit
- Debian GNU / Linux 9.x (Stretch) 32 bit/64 bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 bit
- Ubuntu Server 18.04 LTS (Bionic Beaver) 64 bit
- CentOS 7.x 64 bit
- Red Hat Enterprise Linux Server 8.x 64 bit
- Red Hat Enterprise Linux Server 7.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 1.7 (inclusa la modalità ambiente software chiuso e la modalità obbligatoria) 64 bit
- Astra Linux Special Edition 1.6 (inclusa la modalità ambiente software chiuso e la modalità obbligatoria) 64 bit
- Astra Linux Common Edition 2.12 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
- RED OS 7.3 Server 64 bit
- RED OS 7.3 Certified Edition 64 bit

Sono supportate le seguenti piattaforme di virtualizzazione:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 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
- Macchina virtuale basata su kernel. Supporta i seguenti sistemi operativi:
  - Alt 8 SP Server (LKNV.11100-01) 64-bit
  - Alt Server 10 64-bit
  - Astra Linux Special Edition 1.7 (inclusa la modalità ambiente software chiuso e la modalità obbligatoria) 64 bit
  - Debian GNU/Linux 11.x (Bullseye) 32 bit/64 bit
  - Ubuntu Server 20.04 LTS (Focal Fossa) 64 bit
  - RED OS 7.3 Server 64 bit
  - RED OS 7.3 Certified Edition 64 bit

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 10.5.x 32 bit/64 bit
- MariaDB 10.4.x 32 bit/64 bit
- MariaDB 10.3.22 e versioni successive 32 bit/64 bit
- Server MariaDB 10.3 a 32 bit/64 bit con motore di archiviazione InnoDB
- MariaDB 10.1.30 e versioni successive 32 bit/64 bit

Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console Server

Requisiti hardware insufficienti:

- CPU: 4 core, frequenza operativa di 2,5 GHz.
- RAM: 8 GB.
- Spazio disponibile su disco: 40 GB.

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

- Debian GNU/Linux 11.x (Bullseye)
- Debian GNU/Linux 10.x (Buster)
- Debian GNU/Linux 9.x (Stretch)
- Ubuntu Server 20.04 LTS (Focal Fossa)
- Ubuntu Server 18.04 LTS (Bionic Beaver)
- CentOS 7.x
- Red Hat Enterprise Linux Server 8.x

- Red Hat Enterprise Linux Server 7.x
- SUSE Linux Enterprise Server 12 (tutti i Service Pack)
- SUSE Linux Enterprise Server 15 (tutti i Service Pack)
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 bit
- Astra Linux Special Edition 1.7 (inclusa la modalità ambiente software chiuso e la modalità obbligatoria)
- Astra Linux Special Edition 1.6 (inclusa la modalità ambiente software chiuso e la modalità obbligatoria)
- Astra Linux Common Edition 2.12
- 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 8
- Oracle Linux 7
- RED OS 7.3 Server
- RED OS 7.3 Certified Edition

Tra le piattaforme di virtualizzazione, la macchina virtuale basata su kernel è supportata per i seguenti sistemi operativi:

- Alt 8 SP Server (LKNV.11100-01) 64-bit
- Alt Server 10 64-bit
- Astra Linux Special Edition 1.7 (inclusa la modalità ambiente software chiuso e la modalità obbligatoria) 64 bit
- Debian GNU/Linux 11.x (Bullseye) 32 bit/64 bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 64 bit
- RED OS 7.3 Server 64 bit
- RED OS 7.3 Certified Edition 64 bit

Dispositivi client

Per un dispositivo client, l'utilizzo di Kaspersky Security Center 14 Web Console richiede solo un browser.

I requisiti hardware e software relativi al dispositivo sono identici a quelli del browser utilizzato per Kaspersky Security Center 14 Web Console.

Browser:

- Mozilla Firefox Extended Support versione 91.8.0 o successiva (91.8.0 rilasciata il 5 aprile 2022)
- Mozilla Firefox versione 99.0 o successiva (99.0 rilasciata il 5 aprile 2022)
- Google Chrome 100.0.4896.88 o versioni successive (build ufficiale)
- Microsoft Edge 100 o versioni successive
- Safari 15 su macOS

Network Agent

Requisiti hardware insufficienti:

- 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:

- Debian GNU/Linux 11.x (Bullseye) 32 bit/64 bit
- Debian GNU/Linux 10.x (Buster) 32-bit/64-bit
- Debian GNU / Linux 9.x (Stretch) 32 bit/64 bit
- Ubuntu Server 20.04 LTS (Focal Fossa) 32 bit/64 bit
- Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 bit
- Ubuntu Server 18.04 LTS (Bionic Beaver) 32 bit / 64 bit
- Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 bit / 64 bit
- Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 bit / 64 bit
- CentOS 8.x 64 bit
- CentOS 7.x 64 bit
- CentOS 7.x ARM 64 bit
- Red Hat Enterprise Linux Server 8.x 64 bit
- Red Hat Enterprise Linux Server 7.x 64 bit
- Red Hat Enterprise Linux Server 6.x 32 bit/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 (tutti i Service Pack) 64 bit
- SUSE Linux Enterprise Desktop 15 (Service Pack 3) ARM 64 bit
- openSUSE 15 64 bit
- EulerOS 2.0 SP8 ARM
- Pardus OS 19.1 64 bit
- Astra Linux Special Edition 1.7 (inclusa la modalità ambiente software chiuso e la modalità obbligatoria) 64 bit
- Astra Linux Special Edition 1.6 (inclusa la modalità ambiente software chiuso e la modalità obbligatoria) 64 bit
- Astra Linux Common Edition 2.12 64 bit
- Astra Linux Special Edition 4.7 ARM
- Alt Server 10 64-bit
- Alt Server 9,2 64-bit
- Alt Workstation 10 32 bit/64 bit
- Alt Workstation 9,2 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
- Linux Mint 19.x 32 bit
- Linux Mint 20.x 64 bit
- AlterOS 7.5 e versioni successive a 64 bit
- GosLinux IC6 64 bit
- RED OS 7.3 64 bit
- RED OS 7.3 Server 64 bit
- RED OS 7.3 Certified Edition 64 bit
- ROSA Enterprise Linux Server 7.3 64 bit
- ROSA Enterprise Linux Desktop 7.3 64 bit
- ROSA COBALT Workstation 7.3 64 bit
- ROSA COBALT Server 7.3 64 bit
- Lotos (versione core Linux 4.19.50, DE: MATE) 64 bit

Sono supportate le seguenti piattaforme di virtualizzazione:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 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
- Macchina virtuale basata su kernel. Supporta i seguenti sistemi operativi:
  - Alt 8 SP Server (LKNV.11100-01) 64-bit
  - Alt Server 10 64-bit
  - Astra Linux Special Edition 1.7 (inclusa la modalità ambiente software chiuso e la modalità obbligatoria) 64 bit
  - Debian GNU/Linux 11.x (Bullseye) 32 bit/64 bit
  - Ubuntu Server 20.04 LTS (Focal Fossa) 64 bit
  - RED OS 7.3 64 bit
  - RED OS 7.3 Server 64 bit
  - RED OS 7.3 Certified Edition 64 bit

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

Informazioni di Kaspersky Security Center 14 Web Console

Kaspersky Security Center 14 Web Console è un'applicazione Web progettata per gestire lo stato del sistema di protezione della rete protetta dalle applicazioni Kaspersky.

Utilizzando l'applicazione è possibile eseguire le seguenti operazioni:

- Gestire lo stato del sistema di protezione dell'organizzazione.
- Installare le applicazioni Kaspersky nei dispositivi della rete e gestire le applicazioni installate.
- Gestire i criteri creati per i dispositivi della rete.
- Gestire account utente.
- Gestire le attività per le applicazioni installate nei dispositivi della rete.
- Visualizzare i rapporti sullo stato del sistema di protezione.
- Gestire l'invio dei rapporti ad amministratori di sistema e altri esperti IT.

Kaspersky Security Center 14 Web Console fornisce un'interfaccia Web che assicura l'interazione tra il dispositivo e Administration Server tramite un browser. Administration Server è un'applicazione progettata per la gestione delle applicazioni Kaspersky installate nei dispositivi della rete. Administration Server si connette ai dispositivi della rete attraverso canali protetti con SSL (Secure Sockets Layer). Quando si esegue la connessione a Kaspersky Security Center 14 Web Console utilizzando il browser, questo stabilisce una connessione con Kaspersky Security Center 14 Web Console Server.

I prerequisiti per utilizzare Kaspersky Security Center 14 Web Console sono:

1. Utilizzare un browser per connettersi a Kaspersky Security Center 14 Web Console in cui venga visualizzata l'interfaccia del portale Web.
2. Utilizzare i controlli del portale Web per scegliere il comando da eseguire. Kaspersky Security Center 14 Web Console esegue le seguenti operazioni:
    - Se si seleziona un comando per la ricezione di informazioni (ad esempio, per visualizzare un elenco di dispositivi), Kaspersky Security Center 14 Web Console genera una richiesta di informazioni ad Administration Server, riceve i dati necessari e li invia al browser in un formato semplice da visualizzare.
    - Se è stato scelto un comando di gestione (ad esempio, l'installazione remota di un'applicazione), Kaspersky Security Center 14 Web Console riceve il comando dal browser e lo invia ad Administration Server. L'applicazione riceve il risultato da Administration Server e lo invia al browser in un formato semplice da visualizzare.

Kaspersky Security Center 14 Web Console è un'applicazione multilingue. È possibile modificare la lingua dell'interfaccia in qualsiasi momento, senza riaprire l'applicazione. Quando si installa Kaspersky Security Center 14 Web Console insieme a Kaspersky Security Center, Kaspersky Security Center 14 Web Console ha la stessa lingua di interfaccia del file di installazione. Quando si installa solo Kaspersky Security Center 14 Web Console, l'applicazione ha la stessa lingua di interfaccia del sistema operativo. Se Kaspersky Security Center 14 Web Console non supporta la lingua del file di installazione o del sistema operativo, viene utilizzato l'inglese per impostazione predefinita.

Elenco delle applicazioni Kaspersky supportate

Kaspersky Security Center Linux supporta la distribuzione e la gestione centralizzate di Kaspersky Endpoint Security for Linux. Questa applicazione consente di proteggere sia le workstation che i file server. Fare riferimento alla pagina Web del ciclo di vita di supporto del prodotto per le versioni delle applicazioni.

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.

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	
	Soluzione basata su Windows	Soluzione basata su 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	Windows o Linux
Gerarchia di Administration server	✓	✓
Gerarchia di gruppi di amministrazione	✓	✓
Polling della rete	✓	✓ (solo per intervalli IP)
Numero massimo di dispositivi gestiti	100000	20000
Protezione dei dispositivi gestiti Windows, macOS e Linux	✓	— (solo protezione dei dispositivi 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	✓	✓
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	✓	✓
Monitoraggio dello stato di criteri e attività	✓	✓
Distribuzione del cluster di failover Kaspersky	✓	✓

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 "Kaspersky Security Center Administration Server"
- Impostato per l'avvio automatico all'avvio del sistema operativo
- Con l'account **LocalSystem** o l'account utente selezionato durante l'installazione di Administration Server

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 14 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 14 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 14 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.

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

In una gerarchia, Kaspersky Security Center Linux Administration Server può funzionare solo come server secondario gestito da un Administration Server primario di Kaspersky Security Center basato su Windows o Kaspersky Security Center Cloud Console.

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.
- Modalità di utilizzo di Kaspersky Security Center da parte dei provider di servizi. Un provider di servizi deve installare soltanto Kaspersky Security Center e Kaspersky Security Center 14 Web Console. Per gestire numerosi dispositivi client di varie organizzazioni, un provider di servizi può aggiungere Administration 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.

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. Network Agent deve essere installato in tutti i dispositivi in cui viene utilizzato Kaspersky Security Center per gestire applicazioni Kaspersky.

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

- Con il nome "Kaspersky Security Center 14 Linux Network Agent"
- Impostato per l'avvio automatico all'avvio del sistema operativo

- Utilizzo dell'account LocalSystem

Un dispositivo con Network Agent installato è denominato *dispositivo gestito* o *dispositivo*. È possibile installare Network Agent da una delle seguenti origini:

- Pacchetto di installazione nell'archivio di Administration Server (è necessario avere installato Administration Server)
- Pacchetto di installazione collocato nei server Web Kaspersky

Non è necessario installare Network Agent nel dispositivo in cui è installato Administration Server, perché la versione server di Network Agent viene installata automaticamente insieme ad Administration Server.

I nomi del processo avviato da Network Agent sono i seguenti:

- klnagent64.service (per un sistema operativo a 64 bit)
- klnagent.service (per un sistema operativo a 32 bit)

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.

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 computer del dipendente dal gruppo di amministrazione Contabilità al gruppo di amministrazione Sviluppatori. Il computer riceverà automaticamente le impostazioni dell'applicazione necessarie per gli sviluppatori.

Dispositivo gestito

Un *dispositivo gestito* è un computer che esegue Linux 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 di amministrazione

I dispositivi in cui è installato Kaspersky Security Center 14 Web Console Server sono denominati *workstation di amministrazione*. 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 di amministrazione. Da qualsiasi workstation di amministrazione è possibile gestire contemporaneamente i gruppi di amministrazione di diversi Administration Server in rete. Una workstation di amministrazione può essere connessa a un Administration Server (fisico o virtuale) a qualsiasi livello di gerarchia.

È possibile includere una workstation di amministrazione 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 di amministrazione.

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 14 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 14 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 clienti 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 14 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 figlio.

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 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 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
- Creazione di un pacchetto di installazione basato su un'immagine del sistema operativo di un dispositivo di riferimento

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 14 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, 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 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.

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 (vedere la figura seguente) 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.

Criteri e impostazioni locali delle applicazioni

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. 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 individuazione dispositivi 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.

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 incidente con il livello di importanza *Avviso*. L'incidente sarà pubblicato nelle proprietà del dispositivo, nella sezione **Incidenti**.

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.

Licensing

In questa sezione vengono fornite informazioni sulle condizioni generali relative alle licenze di Kaspersky Security Center 14 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.

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.

Quando si installa Network Agent per Linux, il Contratto di licenza con l'utente finale per Network Agent viene visualizzato in lingua inglese. È possibile consultare il Contratto di licenza con l'utente finale per Network Agent in altre lingue nella cartella /opt/kaspersky/klnagent64/share/license prima di accettare i termini del Contratto di licenza con l'utente finale durante l'installazione.

- 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.

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 l'applicazione, in conformità con i termini del Contratto di licenza con l'utente finale.

Una licenza consente di usufruire dei seguenti tipi di servizi:

- Utilizzo dell'applicazione in conformità alle condizioni del Contratto di licenza con l'utente finale
- Come ottenere assistenza tecnica

L'ambito dei servizi forniti e il periodo di validità per l'utilizzo dell'applicazione dipendono dal tipo di 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 della 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 attivare l'applicazione con la licenza di prova solo una volta.

- *Commerciale* – una licenza a pagamento fornita con l'acquisto dell'applicazione.

  Alla scadenza della licenza commerciale, l'applicazione continua a essere eseguita con funzionalità limitate (ad esempio, gli aggiornamenti dei database di Kaspersky Security Center non sono disponibili). Per continuare a utilizzare tutte le funzionalità di Kaspersky Security Center, è necessario rinnovare la licenza commerciale.

È consigliabile rinnovare la licenza prima della scadenza per assicurare la massima protezione da tutti i tipi di minacce.

Informazioni sul certificato di licenza

Certificato di licenza: 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 dell'installazione di Kaspersky Security Center.
- Il testo dell'Informativa sulla privacy è incluso nel file license.txt, nella cartella di installazione di Kaspersky Security Center.
- 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.

Sono disponibili le seguenti funzioni:

- Creazione di Administration Server virtuali per gestire una rete di filiali remote o organizzazioni client.
- Creazione di una gerarchia di gruppi di amministrazione per gestire dispositivi specifici come una singola entità.
- Controllo dello stato della protezione anti-virus di un'organizzazione.
- Installazione remota delle applicazioni.
- Visualizzazione dell'elenco delle immagini dei sistemi operativi disponibili per l'installazione remota.
- Configurazione centralizzata delle applicazioni installate nei dispositivi client.
- Visualizzazione e modifica di gruppi di applicazioni concesse in licenza esistenti.
- Statistiche e rapporti sul funzionamento dell'applicazione e notifiche sugli eventi critici.
- Visualizzazione e modifica manuale dell'elenco di componenti hardware rilevati dal polling della rete.
- Operazioni centralizzate con file spostati in Quarantena o Backup e file la cui elaborazione è stata rimandata.
- Gestione dei ruoli utente.

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 trasferiti al Titolare dei diritti

Specificati nel Contratto di licenza con l'utente finale di Kaspersky Security Center 14 Linux.

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 in seguito all'individuazione dei dispositivi nella rete oppure tramite la scansione degli intervalli IP. Administration Server acquisisce i dati in modo autonomo o riceve i dati da Network Agent.
- 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 14 Web Console:
    - Specifiche tecniche del dispositivo gestito e relativi componenti richiesti per l'identificazione del dispositivo: nome visualizzato e descrizione del dispositivo, dominio DNS e nome DNS, indirizzo IPv4, indirizzo IPv6, 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, tipo di macchina virtuale (se il dispositivo è una macchina virtuale).
    - 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.
- 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 14 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 aggiuntiva, 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 14 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 14 Web Console.
- Dati elaborati dalla funzionalità Vulnerability e Patch Management. Network Agent trasferisce dal dispositivo ad Administration Server le informazioni sull'hardware rilevato nei dispositivi gestiti (Registro hardware).
- Categorie utente di applicazioni. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center 14 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.
- 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.
- 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.
- Dettagli dei codici di attivazione inseriti. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center 14 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 14 Web Console.
- Cronologia delle revisioni degli oggetti di gestione. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center 14 Web Console.
- Registro degli oggetti di gestione dettagliati. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center 14 Web Console.
- Pacchetti di installazione creati dal file, nonché impostazioni di installazione. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center 14 Web Console.
- Dati necessari per la visualizzazione degli annunci di Kaspersky in Kaspersky Security Center 14 Web Console. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center 14 Web Console.
- Dati necessari per il funzionamento dei plug-in delle applicazioni gestite in Kaspersky Security Center 14 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 14 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 14 Web Console.
- Registro eventi Kaspersky per i componenti Kaspersky Security Center Linux e per le applicazioni Kaspersky gestite. Il registro eventi Kaspersky viene archiviato in ciascun dispositivo e non viene mai trasferito ad Administration Server.
- 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 14 Web Console.
- I dati di Administration Server che l'Utente immette in Kaspersky Security Center 14 Web Console.
- Tutti i dati che l'Utente immette nell'interfaccia di Kaspersky Security Center 14 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 14 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 e Network Agent assegnati a un punto di distribuzione ricevono le informazioni sui dispositivi della rete.

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.

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 14 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. È possibile rinnovare l'abbonamento nel sito Web del provider di servizi.

Eventi di superamento del limite di licenze

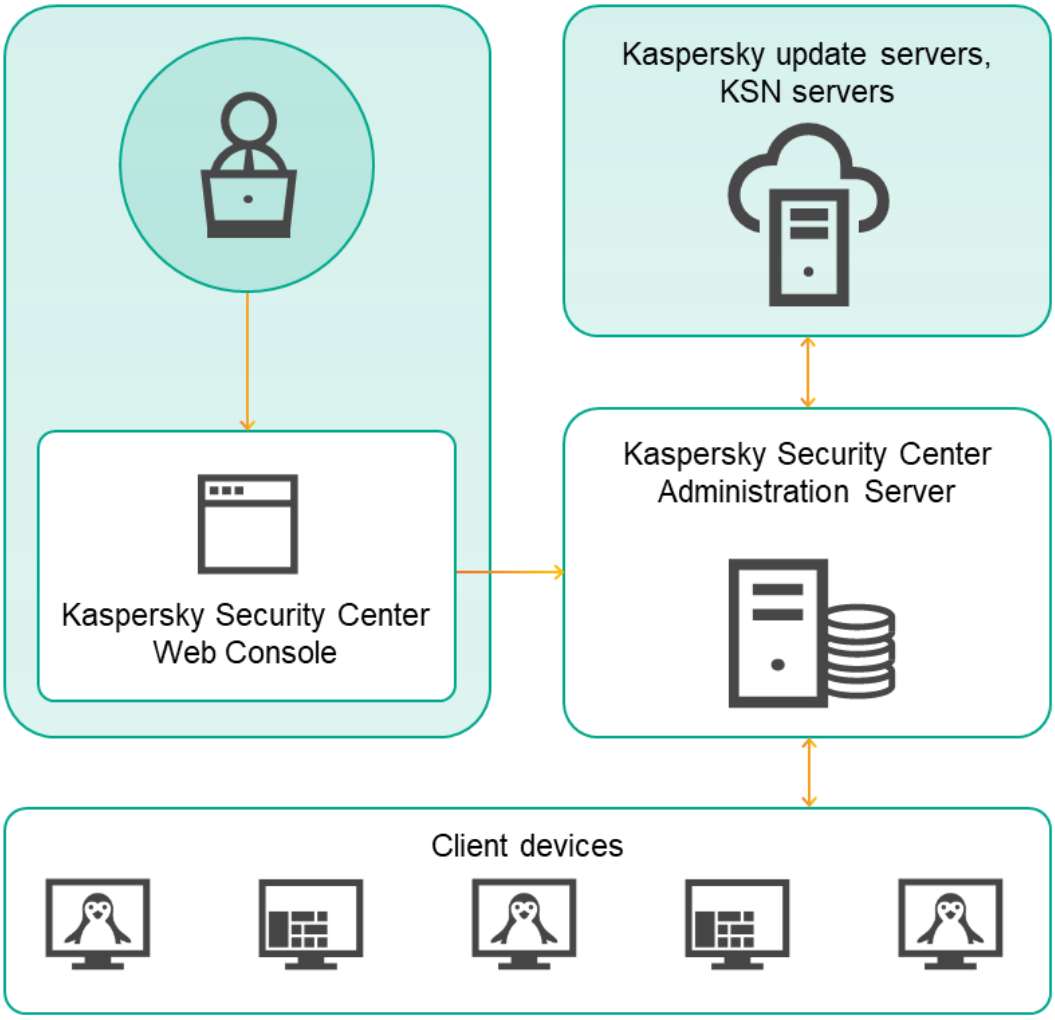
Kaspersky Security Center Linux consente di ottenere informazioni sugli eventi che si verificano in caso di superamento dei limiti di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client.

Il livello di importanza degli eventi quando avviene il superamento di una limitazione di licenza 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**.

Architettura

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



Architettura di Kaspersky Security Center 14 Linux

Kaspersky Security Center 14 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 14 Linux. Ogni dispositivo che deve essere protetto deve avere una delle applicazioni di protezione Kaspersky installate.

Diagramma di distribuzione di Kaspersky Security Center Administration Server e Kaspersky Security Center 14 Web Console

La figura seguente mostra il diagramma di distribuzione di Kaspersky Security Center Administration Server e Kaspersky Security Center 14 Web Console.

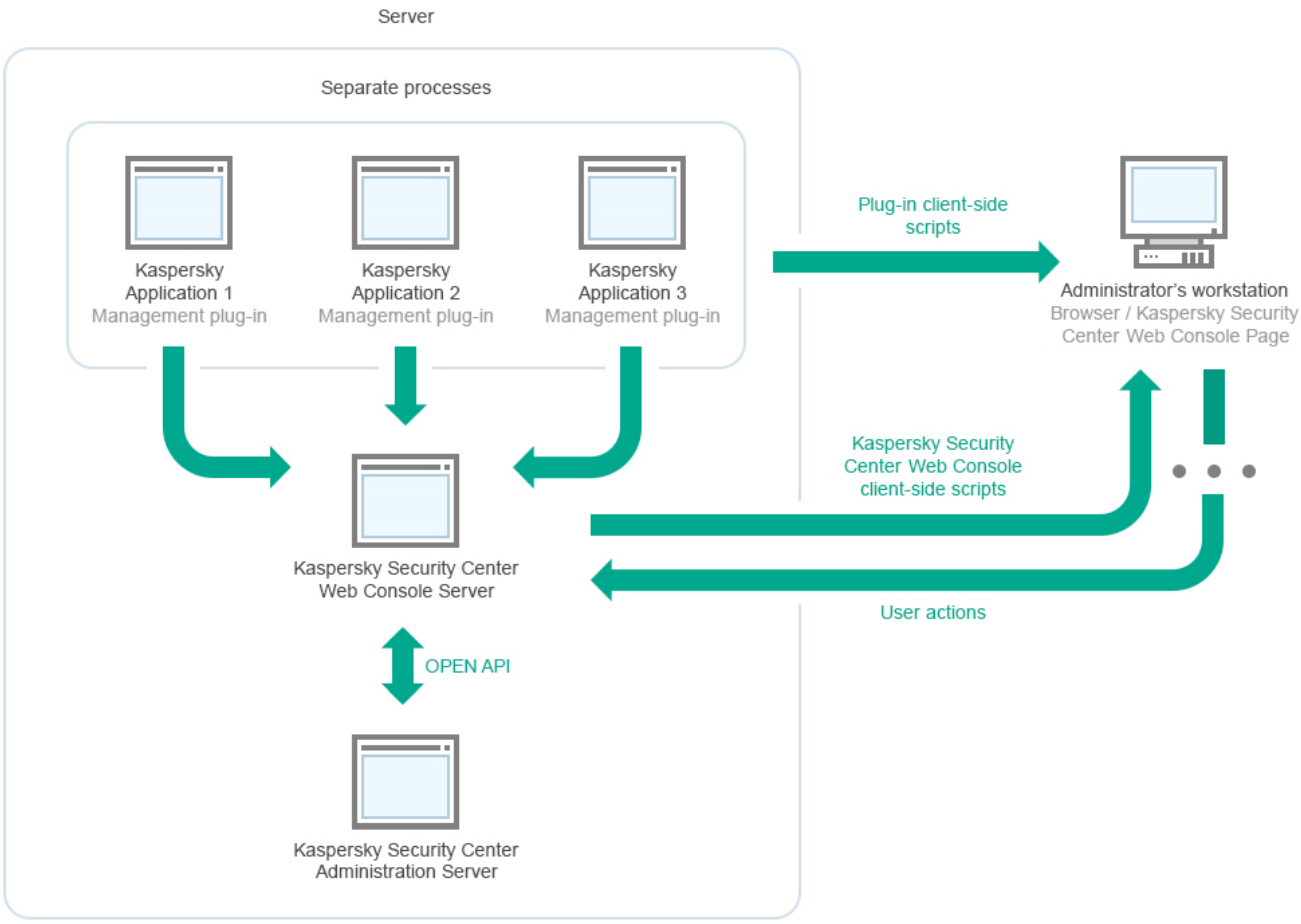


Diagramma di distribuzione di Kaspersky Security Center Administration Server e Kaspersky Security Center 14 Web Console

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 14 Web Console Server.

Come amministratore, accedere a Kaspersky Security Center 14 Web Console utilizzando un browser sulla workstation.

Quando si eseguono azioni specifiche in Kaspersky Security Center 14 Web Console, Kaspersky Security Center 14 Web Console Server comunica con Kaspersky Security Center Administration Server tramite OpenAPI. Kaspersky Security Center 14 Web Console Server richiede le informazioni necessarie a Kaspersky Security Center Administration Server e visualizza i risultati delle operazioni in Kaspersky Security Center 14 Web Console.

Porte utilizzate da Kaspersky Security Center Linux

Nelle seguenti tabelle sono elencate le porte predefinite che devono essere aperte nell'Administration Server e nei 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 che apre la porta	Protocollo	Ambito della porta	Ambito
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** della finestra delle proprietà di Administration Server.
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** della finestra delle proprietà di Administration 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	Gestione dei dispositivi client e degli Administration Server secondari.

			esempio, se l'Administration Server secondario è nella rete perimetrale)	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.
13299	klserver	TCP (TLS)	Ricezione delle connessioni da Kaspersky Security Center 14 Web Console ad Administration Server; ricezione delle connessioni ad Administration Server tramite OpenAPI	Kaspersky Security Center 14 Web Console, 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.
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 dell'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 dell'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**).
19170	klserver	HTTPS (TLS)	Tunneling delle connessioni ai dispositivi gestiti tramite l'utilità klsctunnel	Connessione remota ai dispositivi gestiti tramite Kaspersky Security Center 14 Web Console. È possibile modificare il numero di porta predefinito utilizzando l'utilità klscflag.

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 il server MariaDB). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

La tabella seguente mostra la porta che deve essere aperta in Kaspersky Security Center Linux Web Console Server. Può trattarsi dello stesso dispositivo in cui è installato Administration Server o di un dispositivo diverso.

Porta utilizzata da Kaspersky Security Center Linux 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 14 Web Console	Kaspersky Security Center 14 Web Console. È possibile modificare il numero di porta predefinito durante l'installazione di Kaspersky Security Center 14 Web Console. Se si installa Kaspersky Security Center 14 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 che deve essere aperta nei 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 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.

La tabella seguente mostra le porte che devono essere aperte in 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 devono essere aperte nei 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 delle connessioni dai Network Agent	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.

Porte utilizzate da Kaspersky Security Center 14 Web Console

La tabella seguente elenca le porte che devono essere aperte nel dispositivo in cui è installato Kaspersky Security Center 14 Web Console Server (noto anche come Kaspersky Security Center 14 Web Console).

Porte utilizzate da Kaspersky Security Center 14 Web Console

Numero di porta	Nome servizio	Protocollo	Ambito della porta	Ambito
2001	KSCWebConsolePlugin	HTTPS	Porta API utilizzata dai processi del plug-in di gestione per ricevere richieste da KSCWebConsoleManagementService	Esecuzione dei processi node.exe dei plug-in di gestione
1329, 2003	KSCWebConsoleManagementService	HTTPS	Porte API utilizzate per ricevere richieste dal servizio KSCWebConsole in esecuzione nello stesso dispositivo	Aggiornamento dei componenti di Kaspersky Security Center 14 Web Console
2005	KSCWebConsole	HTTPS	Porta API utilizzata per ricevere richieste dal servizio KSCWebConsoleManagementService in esecuzione nello stesso dispositivo	Esecuzione dei processi node.exe di Kaspersky Security Center 14 Web Console
8200	—	HTTP	Porta API utilizzata per generare	Installazione di Kaspersky Security

			certificati tramite HashiCorp Vault (per maggiori dettagli, consultare il sito Web di HashiCorp Vault)	Center 14 Web Console e aggiornamento dei componenti di Kaspersky Security Center 14 Web Console
4150, 4151, 4152	KSCWebConsoleMessageQueue	HTTPS	Porte API del broker di messaggi utilizzate per la comunicazione tra i processi di Kaspersky Security Center 14 Web Console e dei plug-in di gestione	Interazione tra Kaspersky Security Center 14 Web Console e plug-in di gestione

Installazione

Questa sezione descrive l'installazione di Kaspersky Security Center e Kaspersky Security Center 14 Web Console.

Scenario di installazione principale

Tramite questo scenario è possibile installare Kaspersky Security Center 14 Linux Administration Server e Kaspersky Security Center 14 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 14 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 o utilizzarne uno esistente.

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**

   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 nel dispositivo. La versione server di Network Agent è installata automaticamente insieme ad Administration Server.

6. **Installazione di Kaspersky Security Center 14 Web Console e dei plug-in Web di gestione**

   Selezionare un dispositivo Linux che si intende utilizzare come workstation di amministrazione, assicurarsi che il dispositivo soddisfi i requisiti software e hardware, quindi installare Kaspersky Security Center 14 Web Console nel dispositivo. È possibile installare Kaspersky Security Center 14 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 14 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 l'individuazione dispositivi, 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 di 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 l'individuazione dei dispositivi.

    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 di 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 di un sistema di gestione database

Installare il sistema di gestione database (DBMS) che verrà utilizzato da Kaspersky Security Center. È possibile scegliere uno dei DBMS supportati.

Per informazioni su come installare il DBMS selezionato, consultare la relativa documentazione.

Se si utilizza MariaDB, è necessario configurare le impostazioni consigliate per il funzionamento ottimale del DBMS con Kaspersky Security Center.

Configurazione del server MariaDB x64 per l'utilizzo con Kaspersky Security Center 14 Linux

Se utilizzi il server MariaDB per Kaspersky Security Center, abilita 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 configurare il file my.cnf:

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

2. Immettere le seguenti righe nel 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.

   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.

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.

Installazione di Kaspersky Security Center

Questa procedura descrive come installare Kaspersky Security Center.

Prima dell'installazione:

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

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:

1. Nella riga di comando eseguire i comandi presenti in questa istruzione con un account con privilegi di root.

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

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

4. Eseguire la configurazione di Kaspersky Security Center:

   ```
   # /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 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 è necessario accettare i termini dell'Informativa sulla privacy.

6. 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 non può contenere meno di 8 o più 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 (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

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

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 14 Web Console

Questa sezione descrive come installare Kaspersky Security Center 14 Web Console Server (anche noto come Kaspersky Security Center 14 Web Console) nei dispositivi che eseguono il sistema operativo Linux. Prima dell'installazione, è necessario installare un sistema di gestione database e Kaspersky Security Center Administration Server.

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 14 Web Console:

1. Verificare che il dispositivo in cui si desidera installare Kaspersky Security Center 14 Web Console esegua una delle distribuzioni Linux supportate.
2. Leggere il Contratto di licenza con l'utente finale (EULA) nel pacchetto di installazione (file /var/opt/kaspersky/ksc-web-console/license-<XX>.txt, dove<XX> è un codice lingua). 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 14 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:

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

   Quando si installa Kaspersky Security Center 14 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 14 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 14 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 14 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 14 Web Console è installato nella seguente directory: /var/opt/kaspersky/ksc-web-console.

5. Riavviare tutti i servizi Kaspersky Security Center 14 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 14 Web Console.

Parametri di installazione di Kaspersky Security Center 14 Web Console

Per installare Kaspersky Security Center 14 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 14 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:

```
{
  "indirizzo": "127.0.0.1",
  "porta": 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”: “Gruppo1:Utente1",
  “managementServiceAccount”: “Gruppo1:Utente2",
  “serviceWebConsoleAccount”: “ Gruppo1:Utente3 ”,
  "pluginAccount": "Gruppo1:Utente4",
  “messageQueueAccount": "Gruppo1:Utente5"
}
```

Quando si installa Kaspersky Security Center 14 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 14 Web Console nei dispositivi che eseguono Linux

Parametro	Descrizione	Valori disponibili
`address`	Indirizzo di Kaspersky Security Center 14 Web Console Server (obbligatorio).	Valore stringa.
`port`	Numero della porta utilizzata da Kaspersky Security Center 14 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 14 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 14 Web Console. Ogni Administration Server deve essere definito con i seguenti parametri: • Indirizzo di Administration Server • Porta OpenAPI utilizzata da Kaspersky Security Center 14 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`: ho letto, compreso e accettato i termini del Contratto di licenza con l'utente finale. • `false`: non accetto i termini del Contratto di licenza (selezionato per impostazione predefinita).
`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 KSCWebConsole.	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 14 Web Console crea un nuovo account con il nome predefinito `user_management_%uid%`.
`managementServiceAccount`	Nome dell'account con privilegi con cui viene eseguito il servizio KSCWebConsoleManagement.	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 14 Web Console crea un nuovo account con il nome predefinito `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Nome dell'account con cui viene eseguito il servizio KSCSvcWebConsole.	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 14 Web Console crea un nuovo account con il nome predefinito `user_svc_nodejs_%uid%`.
`pluginAccount`	Nome dell'account con cui viene eseguito il servizio KSCWebConsolePlugin.	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 14 Web Console crea un nuovo account con il nome predefinito `user_web_plugin_%uid%`.
`messageQueueAccount`	Nome dell'account con cui viene eseguito il servizio KSCWebConsoleMessageQueue.	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 14 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 14 Web Console crea un gruppo di protezione predefinito, quindi crea account utente con nomi predefiniti in questo gruppo.

Account per l'utilizzo del DBMS

La seguente tabella fornisce informazioni sulle proprietà degli account selezionati per l'utilizzo con il DBMS MariaDB.

Il *DBMS locale* è un DBMS installato nello stesso dispositivo di Administration Server. Il *DBMS remoto* è un DBMS installato in un altro dispositivo.

Concedere tutti i diritti richiesti per l'account di Administration Server prima dell'avvio del servizio di Administration Server.

DBMS: MariaDB

Posizione del DBMS	Locale o remoto.	Locale o remoto.
Chi crea il database KAV	Programma di installazione (automaticamente).	Amministratore (manualmente).
Account con cui viene eseguito il programma di installazione	Locale o di dominio, con diritti di amministratore locale.	Locale o di dominio, con diritti di amministratore locale.
Account del servizio di Administration Server	Locale o dominio.	Locale o dominio.
Diritti dell'account interno DBMS utilizzato dal programma di installazione e dal servizio Administration Server per accedere a DBMS	È richiesto l'accesso radice.	`GRANT ALL` per il database KAV, e `SELECT`, `SHOW VIEW`, `PROCESS` per le tabelle di sistema.

Distribuzione del cluster di failover Kaspersky

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

Scenario: Distribuzione di un cluster di failover Kaspersky

Un cluster di failover Kaspersky garantisce un'elevata disponibilità di Kaspersky Security Center 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 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. **Creazione di un account per i servizi di Kaspersky Security Center**

   Creare un nuovo account utente di dominio o selezionarne uno esistente con il quale verranno eseguiti i servizi di Kaspersky Security Center. Aggiungere l'account selezionato nel gruppo di amministratori locali in ciascuno dei nodi e nel file server.

2. **Preparazione del file server**

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

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

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

   Preparare due computer 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

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

   Sono disponibili due opzioni:

   - Se si desidera utilizzare MariaDB Galera Cluster, non è necessario un computer 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 computer dedicato.

5. **Installazione di Kaspersky Security Center**

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

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 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 di Kaspersky viene distribuito. Familiarizzare con gli eventi che determinano il passaggio dai nodi attivi a quelli passivi.

Informazioni sul cluster di failover di Kaspersky

Un cluster di failover Kaspersky garantisce un'elevata disponibilità di Kaspersky Security Center 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 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 di Kaspersky, tutti i servizi di Kaspersky Security Center vengono gestiti automaticamente. Non tentare di riavviare i servizi manualmente.

Requisiti hardware e software

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

- Due computer con hardware e software identici. Questi computer fungeranno da nodi attivi e passivi.
- Un file server che esegue Linux, con il file system EXT4. È necessario mettere a disposizione un computer 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 computer con DBMS (Database Management System). Se si utilizza MariaDB Galera Cluster come DBMS, non è necessario un computer dedicato per questo scopo.

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 non è riuscito o è stato deliberatamente terminato dall'utente. I servizi di Kaspersky Security Center 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

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

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. Specificare i percorsi delle cartelle condivise durante la configurazione dell'installazione di Kaspersky Security Center.

   Eseguire i seguenti comandi:

   ```
   sudo yum install nfs-utils
   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 cat /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, seguire le istruzioni aggiuntive in questo scenario.

Preparazione dei nodi per un cluster di failover Kaspersky

Preparare due computer affinché fungano da nodi attivi e passivi del cluster di failover Kaspersky.

Per preparare i nodi per il cluster di failover Kaspersky:

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

2. Per utilizzare i nodi come client NFS, installare il pacchetto nfs-utils in ogni nodo.

   Eseguire il seguente comando:

   ```
   sudo yum install nfs-utils
   ```

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

4. Verificare che le cartelle condivise possano essere montate correttamente. [passaggio facoltativo]

   Eseguire i seguenti comandi:

   ```
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,auto,user,rw {server}:{percorso della cartella
   KlFocStateShare} /mnt/KlFocStateShare
   sudo mount -t nfs -o vers=4,nolock,local_lock=none,noauto,user,rw {server}:{percorso della cartella
   KlFocDataShare_klfoc} /mnt/KlFocDataShare_klfoc
   ```

   Qui, `{server}:{percorso della cartella KlFocStateShare}` e `{server}:{percorso della cartella KlFocDataShare_klfoc}` sono i percorsi di rete delle cartelle condivise nel file server.

   Dopo che le cartelle condivise sono state montate correttamente, smontarle eseguendo i seguenti comandi:

   ```
   sudo umount /mnt/KlFocStateShare
   sudo umount /mnt/KlFocDataShare_klfoc
   ```

5. Abbinare i punti di montaggio e le cartelle condivise:
   ```
   sudo vi /etc/fstab
   {server}:{percorso della cartella KlFocStateShare} /mnt/KlFocStateShare nfs
   vers=4,nolock,local_lock=none,auto,user,rw 0 0
   {server}:{percorso della cartella KlFocDataShare_klfoc} /mnt/KlFocDataShare_klfoc nfs
   vers=4,nolock,local_lock=none,noauto,user,rw 0 0
   ```

   Qui, `{server}:{percorso della cartella KlFocStateShare}` e `{server}:{percorso della cartella KlFocDataShare_klfoc}` sono i percorsi di rete delle cartelle condivise nel file server.

6. Riavviare entrambi i nodi.

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

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

   Eseguire il seguente comando:

   ```
   sudo ls -la /mnt/
   ```

9. Eseguire una delle seguenti operazioni:

   - In ogni nodo creare una scheda di rete virtuale. Ad esempio, eseguire i seguenti comandi:

     a. Scoprire i nomi delle interfacce eseguendo il comando seguente:
     ```
     ifconfig
     ```

     b. Eseguire il seguente script (di seguito i nomi delle interfacce sono forniti come esempi):
     ```
     #!/bin/bash
     PHYSICAL_IFACE=ens160
     VIRTUAL_IFACE=macvlan1
     ip link del $VIRTUAL_IFACE > /dev/null 2>&1
     ip link add link $PHYSICAL_IFACE $VIRTUAL_IFACE type macvlan
     if [ "$?" -ne "0" ]; then
         echo ERROR adding new virtual adapter $VIRTUAL_IFACE!
         exit $?
     fi
     ip link set $VIRTUAL_IFACE down
     if [ "$?" -ne "0" ]; then
         echo ERROR disabling virtual adapter $VIRTUAL_IFACE!
         exit $?
     fi
     ```

c. Eseguire il seguente comando:

```
ip addr add {indirizzo IP della scheda di rete virtuale} dev {nome della scheda di rete virtuale}
```

L'indirizzo IP deve essere vuoto quando si crea la scheda di rete virtuale. Le schede di rete virtuali in entrambi i nodi devono avere lo stesso indirizzo IP.

d. Verificare che la scheda di rete virtuale sia stata creata correttamente.

Eseguire i seguenti comandi:

```
ip link set macvlan1 up
ifconfig
```

e. Disabilitare la scheda di rete virtuale eseguendo il comando seguente:

```
ip link set macvlan1 down
```

- 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 computer 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 13291, TCP 13299, TCP 17000.

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

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

Questa procedura descrive come installare Kaspersky Security Center nei nodi del cluster di failover di Kaspersky. Kaspersky Security Center viene installato separatamente in entrambi i nodi del cluster di failover Kaspersky. 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.

Solo un utente del gruppo di domini KLAdmins può installare Kaspersky Security Center in ogni nodo.

Installazione nel nodo primario (attivo)

Per installare Kaspersky Security Center nel nodo primario:

1. Verificare che il dispositivo in cui si desidera installare Kaspersky Security Center esegua una delle distribuzioni Linux supportate.
2. Nella riga di comando eseguire i comandi presenti in questa istruzione con un account con privilegi di root.
3. Eseguire l'installazione di Kaspersky Security Center. 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:

   ```
   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 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 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 virtuale o un servizio di bilanciamento del carico esterno.

d. Se si utilizza una scheda di rete virtuale, 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 virtuale o l'indirizzo IP del servizio di bilanciamento del carico esterno.

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

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

h. 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.

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

j. 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".

k. 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".

l. Immettere 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, viene utilizzata la porta 3306.

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.

Attendere che i servizi vengano aggiunti e avviati automaticamente:

- klnagent_srv
- kladminserver_srv
- klactprx_srv
- klwebsrv_srv

q. 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 nel nodo primario.

Installazione nel nodo secondario (passivo)

Per installare Kaspersky Security Center nel nodo secondario:

1. Verificare che il dispositivo in cui si desidera installare Kaspersky Security Center esegua una delle distribuzioni Linux supportate.
2. Nella riga di comando eseguire i comandi presenti in questa istruzione con un account con privilegi di root.
3. Eseguire l'installazione di Kaspersky Security Center. 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:

   ```
   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 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 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 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 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 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 `detach_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.

Certificati per l'utilizzo di Kaspersky Security Center

Questa sezione contiene informazioni sui certificati di Kaspersky Security Center e descrive come emettere e sostituire certificati per Kaspersky Security Center 14 Web Console e come rinnovare un certificato per Administration Server se il Server interagisce con Kaspersky Security Center 14 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 14 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 14 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.

Certificati di Administration Server

Un certificato Administration Server è necessario per i seguenti scopi:

- Autenticazione di Administration Server durante la connessione a Kaspersky Security Center 14 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 14 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.

> Se si specifica un periodo di validità superiore a 397 giorni per il certificato di Administration Server, il browser Web restituisce un errore.

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.

Certificato Server Web

Uno speciale tipo di certificato viene utilizzato da Server Web, un componente di Kaspersky Security Center Administration Server. 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 14 Web Console
2. Certificato Administration Server comune ("C")

Certificato di Kaspersky Security Center 14 Web Console

Il server di Kaspersky Security Center 14 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

La seguente tabella visualizza i requisiti per i certificati personalizzati specificati per i diversi componenti di Kaspersky Security Center.

Requisiti per i certificati di Kaspersky Security Center

Tipo di certificato	Requisiti	Commenti
Certificato comune, certificato di riserva comune ("C", "CR")	Lunghezza minima della chiave: 2048. Vincoli di base: • CA: true • 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.	Non applicabile.
Certificato di Kaspersky Security Center 14 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 14 Web Console.

Riemissione del certificato per Kaspersky Security Center 14 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 14 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 14 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 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 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 14 Web Console:

Reinstallare Kaspersky Security Center 14 Web Console eseguendo una delle seguenti operazioni:

- Se si desidera utilizzare lo stesso file di installazione di Kaspersky Security Center 14 Web Console, rimuovere Kaspersky Security Center 14 Web Console, quindi installare la stessa versione di Kaspersky Security Center 14 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 14 Web Console viene riemesso per un altro periodo di validità di 397 giorni.

Sostituzione del certificato per Kaspersky Security Center 14 Web Console

Per impostazione predefinita, quando si installa Kaspersky Security Center 14 Web Console Server (anche noto come Kaspersky Security Center 14 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 14 Web Console con uno personalizzato:

1. Creare un nuovo file di risposta richiesto per l'installazione di Kaspersky Security Center 14 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 14 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 14 Web Console, rimuovere Kaspersky Security Center 14 Web Console, quindi installare la stessa versione di Kaspersky Security Center 14 Web Console.
   - Se si desidera utilizzare un file di installazione di una versione aggiornata, eseguire il comando di upgrade.

Kaspersky Security Center 14 Web Console funziona con il certificato specificato.

Conversione di un certificato PFX nel formato PEM

Per utilizzare un certificato PFX in Kaspersky Security Center 14 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 14 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 14 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.

Se si specifica un periodo di validità superiore a 397 giorni per il certificato di Administration Server, il browser Web restituisce un errore.

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. Non è compatibile con le versioni precedenti di Kaspersky Security Center.

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 o il certificato di riserva comune prima della scadenza. 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.
`-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.

Connessione dei Network Agent ad Administration Server con l'utilità klmover

Dopo aver sostituito il certificato di Administration Server utilizzando l'utilità klsetsrvcert della riga di comando, è necessario stabilire la connessione SSL tra Network Agent e Administration Server in quanto la connessione è interrotta.

Per specificare il nuovo certificato di Administration Server e ripristinare la connessione:

Dalla riga di comando eseguire la seguente utilità:

```
klmover [-address <indirizzo server>] [-pn <numero porta>] [-ps <numero porta SSL>] [-nossl] [-cert <percorso del
file di certificato>]
```

Questa utilità viene copiata automaticamente nella cartella di installazione di Network Agent, quando Network Agent viene installato in un dispositivo client.

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.

Informazioni sull'upgrade di Kaspersky Security Center Linux

È possibile installare la versione 14 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 14, tutti i dati e le impostazioni della versione precedente di Administration Server vengono mantenuti.

Durante l'aggiornamento, l'utilizzo simultaneo del DBMS da parte di Administration Server e di un'altra applicazione non è consentito.

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
- Creando il backup dei dati di Administration Server, installando una nuova versione di Administration Server e ripristinando i dati di Administration Server dal backup

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.

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.

Upgrade di Kaspersky Security Center Linux utilizzando il file di installazione

Per aggiornare Administration Server da una versione precedente (a partire dalla versione 13) alla versione 14, è possibile installare una nuova versione su una precedente utilizzando il file di installazione di Kaspersky Security Center.

Per eseguire l'upgrade di una versione precedente di Administration Server alla versione 14 utilizzando il file di installazione:

1. Scaricare il file di installazione di Kaspersky Security Center con un pacchetto completo per la versione 14 dal sito Web di Kaspersky:
   - Per i dispositivi che eseguono un sistema operativo basato su RPM: ksc64—<numero versione> -11247.x86_64.rpm
   - Per i dispositivi che eseguono un sistema operativo basato su Debian—ksc64_<numero versione> -11247_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 rpm -Uvh --nodeps --force ksc64-<numero versione>-11247.x86_64.rpm
     ```

- Per i dispositivi che eseguono un sistema operativo basato su Debian:
  `$ sudo dpkg -i ksc64_<numero versione>-11247_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. 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:

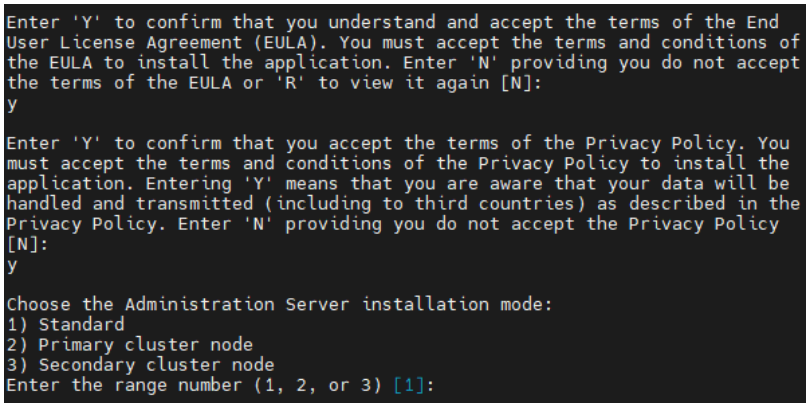
   a. Inserire 'Y' per confermare di aver letto, compreso e accettato i termini e le condizioni dell'EULA.

   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 eseguire l'upgrade di Administration Server da una versione precedente (a partire dalla versione 13) alla versione 14, è possibile creare un backup dei dati di Administration Server e ripristinare questi dati dopo aver installato una nuova versione di Kaspersky Security Center. 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 14 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.
3. Installare Kaspersky Security Center versione 14 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.

Accesso a Kaspersky Security Center 14 Web Console e disconnessione

È possibile accedere a Kaspersky Security Center 14 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 14 Web Console:

1. Nel browser visitare <indirizzo Web di Administration Server>:<numero di porta>.

   Verrà 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, vengono visualizzati solo i campi Nome di accesso e Password.

3. Eseguire una delle seguenti operazioni:

   - Per accedere all'Administration Server fisico, immettere il nome utente e la password dell'amministratore locale.
   - Se nel server vengono creati uno o più Administration Server virtuali e si desidera accedere a un server virtuale:

     a. Fare clic su **Impostazioni avanzate**.

     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.

Dopo l'accesso, viene visualizzato il dashboard, con la lingua e il tema utilizzati l'ultima volta. È possibile spostarsi in Kaspersky Security Center 14 Web Console e utilizzarlo per lavorare con Kaspersky Security Center Linux.

Per eseguire la disconnessione da Kaspersky Security Center 14 Web Console:

1. Fare clic sul nome utente nell'angolo superiore destro dello schermo.
2. Nel menu a discesa selezionare **Esci**.

Kaspersky Security Center 14 Web Console verrà chiuso e sarà visualizzata la pagina di accesso.

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 di notifiche tramite e-mail per informare degli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni gestite (per il corretto invio delle notifiche, il servizio Messenger deve essere in esecuzione in Administration Server e in tutti i dispositivi dei destinatari).
- Creare un criterio di protezione per workstation e server, nonché attività di scansione virus, 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. Nella finestra principale dell'applicazione fare clic sull'icona **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 **Avvia 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

Espandi tutto | Comprimi tutto

Specificare le impostazioni di accesso a Internet per Kaspersky Security Center Linux.

Se si desidera utilizzare un server proxy durante la connessione a Internet, selezionare la casella di controllo **Usa server proxy**. Se questa casella di controllo è selezionata, i campi sono disponibili per l'immissione delle impostazioni. Specificare le seguenti impostazioni per la connessione a un server proxy:

- **Indirizzo**
- **Numero di porta**
- 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 (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata)

  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 (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata)

  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.

Passaggio 2. Selezione del metodo di attivazione dell'applicazione

Espandi tutto | Comprimi tutto

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 con 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 3. 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 4. Configurazione delle notifiche e-mail

Espandi tutto | Comprimi tutto

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. 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 e le impostazioni per l'autenticazione ESMTP non sono disponibili.

È possibile verificare le nuove impostazioni di notifica e-mail facendo clic sul pulsante **Invia messaggio di prova**.

Passaggio 5. 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 i programmi di sicurezza 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.

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 fare clic su **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 1. 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 2. Selezione di un metodo per la distribuzione del file chiave o del codice di attivazione

Espandi tutto | Comprimi tutto

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 i dettagli della chiave di licenza.

Passaggio 3. 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 4. Selezione dei dispositivi

Espandi tutto | Comprimi tutto

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.

- **Seleziona 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 5. Specificazione delle impostazioni dell'attività di installazione remota

Espandi tutto | Comprimi tutto

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 Linux.

  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.

Definire l'impostazione aggiuntiva:

Non installare 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 6. 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 7. Spostamento dei dispositivi in Dispositivi gestiti

Espandi tutto | Comprimi tutto

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 8. Selezione degli account per l'accesso ai dispositivi

Espandi tutto | Comprimi tutto

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)**

  Se questa opzione è selezionata, è possibile specificare l'account con cui verrà eseguito il programma di installazione dell'applicazione. È possibile specificare l'account utente se Network Agent non è stato installato nei dispositivi a cui è assegnata l'attività.

  È possibile specificare più account utente, ad esempio se nessuno di essi dispone di tutti i diritti richiesti per tutti i dispositivi a cui è assegnata l'attività. In questo caso, tutti gli account che sono stati aggiunti vengono utilizzati per l'esecuzione dell'attività, consecutivamente, dall'alto in basso.

  Se non è stato aggiunto alcun account, l'attività sarà eseguita tramite l'account con cui viene eseguito Administration Server.

Passaggio 9. Avvio dell'installazione

Questo è il passaggio finale della procedura guidata. A questo punto, l'**Attività di installazione remota** è stata creata e configurata.

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.

Configurazione di Administration Server

Questa sezione descrive il processo di configurazione e le proprietà di Kaspersky Security Center Linux Administration Server.

Configurazione della connessione di Kaspersky Security Center 14 Web Console ad Administration Server

Per impostare le porte di connessione di Administration Server:

1. Nella parte superiore dello schermo fare clic sull'icona **Impostazioni** ( ) accanto al nome dell'Administration Server desiderato.

   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 accedere a Kaspersky Security Center

Per impostazione predefinita, gli utenti possono accedere a Kaspersky Security Center da qualsiasi dispositivo in cui possono aprire Kaspersky Security Center 14 Web Console (di seguito denominato Web Console). Tuttavia, è possibile configurare Administration Server in modo che gli utenti possano connettersi ad esso solo da dispositivi con indirizzi IP consentiti. In questo caso, anche se un utente malintenzionato ruba un account Kaspersky Security Center, egli non sarà in grado di accedere a Kaspersky Security Center perché l'indirizzo IP del suo dispositivo non è presente nella lista consentiti.

L'indirizzo IP viene verificato quando un utente accede a Kaspersky Security Center o esegue un'applicazione che interagisce con Administration Server tramite Kaspersky Security Center OpenAPI. In questo momento, il dispositivo di un utente 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:

- Web Console Server

  Se si accede a Kaspersky Security Center tramite Web Console, è possibile configurare un firewall nel dispositivo in cui è installato Web Console Server utilizzando le modalità standard del sistema operativo. Se quindi qualcuno tenta di accedere a Kaspersky Security Center in un dispositivo e 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:

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 (in genere, /opt/kaspersky/ksc64/sbin).
3. Immettere il comando seguente, utilizzando i diritti di amministratore:
   `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 nel prompt dei comandi, utilizzando i diritti di amministratore:
   `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.

Visualizzazione del registro delle connessioni all'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. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** ( ) accanto al nome dell'Administration Server desiderato.

   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 %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Impostazione del numero massimo di eventi nell'archivio eventi

Nella sezione **Archivio eventi** della finestra delle proprietà dell'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.

Se il numero di eventi nel database raggiunge il valore massimo specificato dall'amministratore, l'applicazione elimina gli eventi meno recenti e li sovrascrive con quelli nuovi. Quando l'Administration Server elimina gli eventi meno recenti, non può salvare i nuovi eventi nel database. Durante questo periodo di tempo, le informazioni sugli eventi rifiutati vengono scritte nel registro eventi Kaspersky. I nuovi eventi vengono accodati e quindi salvati nel database al termine dell'operazione di eliminazione.

Per limitare il numero di eventi che è possibile archiviare nell'archivio eventi di Administration Server:

1. Nella parte superiore dello schermo fare clic sull'icona **Impostazioni** ( ) accanto al nome dell'Administration Server desiderato.

   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**.

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. Utilizzando i backup è possibile ripristinare i dati durante lo spostamento del database di un Administration Server in un altro dispositivo o nel corso dell'aggiornamento a una versione più recente di Kaspersky Security Center.

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.

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 14 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. Accedere a **DISPOSITIVI → ATTIVITÀ**.
2. Fare clic su **Aggiungi**.

   Verrà avviata l'Aggiunta guidata attività.
3. Nell'elenco **Applicazione** della prima pagina della procedura guidata selezionare **Kaspersky Security Center 14** e nell'elenco **Tipo di attività** selezionare **Backup dei dati di Administration Server**.
4. Nella pagina corrispondente della procedura guidata specificare le seguenti impostazioni:
   - Cartella per l'archiviazione delle copie di backup
   - Password per il backup (opzionale)
   - Numero massimo di copie di backup da salvare
5. Se nella pagina **Completare la creazione dell'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.

Utilità per il backup e il ripristino dei dati (klbackup)

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'utilità klbackup può essere eseguita in due modalità:

- Interattiva
- Non interattiva

Backup e ripristino dei dati in modalità interattiva

Espandi tutto | Comprimi tutto

Per creare una copia di backup dei dati di Administration Server in modalità interattiva:

1. Eseguire l'utilità klbackup ubicata nella cartella di installazione di Kaspersky Security Center (in genere, /opt/kaspersky/ksc64/sbin/klbackup).

   Verrà avviata la Procedura guidata di backup e ripristino.
2. Nella prima finestra della procedura guidata selezionare **Esegui il backup dei dati di Administration Server**.

   Se si seleziona l'opzione **Esegui il ripristino o il backup solo del certificato di Administration Server**, verrà salvata solo una copia di backup del certificato di Administration Server.

   Fare clic su **Avanti**.
3. Nella finestra successiva della procedura guidata specificare una password e una cartella di destinazione per il backup, quindi fare clic sul pulsante **Avanti** per avviare il backup.

Per ripristinare i dati di Administration Server in modalità interattiva:

1. Eseguire l'utilità klbackup ubicata nella cartella di installazione di Kaspersky Security Center (in genere, /opt/kaspersky/ksc64/sbin/klbackup). Avviare klbackup con lo stesso account utilizzato per l'installazione di Administration Server.

   Verrà avviata la Procedura guidata di backup e ripristino.
2. Nella prima finestra della procedura guidata selezionare **Ripristina dati di Administration Server**.

   Se si seleziona l'opzione **Esegui il ripristino o il backup solo del certificato di Administration Server**, il certificato di Administration Server verrà solo ripristinato.

   Fare clic su **Avanti**.

3. Nella finestra **Ripristinare le impostazioni** della procedura guidata:

   - Specificare la cartella che contiene una copia di backup dei dati di Administration Server. È necessario assicurarsi che il file si chiami backup.zip.
   - Specificare la password che è stata immessa durante il backup dei dati.

     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.

4. Fare clic sul pulsante **Avanti** per ripristinare i dati.

Backup e ripristino dei dati in modalità non interattiva

Per creare una copia di backup o eseguire il ripristino dei dati di Administration Server in modalità non interattiva:

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

> 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).
- `-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` – Durante il salvataggio dei dati, copiare le informazioni nella cartella BACKUP_PATH in una sottocartella con un nome che contiene la data di sistema corrente e l'ora dell'operazione nel formato `klbackup YYYY-MM-DD # HH-MM-SS`. 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 `C:\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` – Salvare o recuperare il certificato dell'Administration Server; per criptare e decriptare il certificato, utilizzare la password specificata dal parametro PASSWORD.

  > 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.
- `-online` – Eseguire il backup dei dati dell'Administration Server creando uno snapshot del volume per ridurre al minimo il tempo offline dell'Administration Server. Quando si utilizza l'utilità per recuperare i dati, questa opzione viene ignorata.

Spostamento di Administration Server e di un server di database 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

- 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 14 Web Console o eseguire l'utilità klbackup.

2. 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 14 Web Console e Network Agent. Controllare inoltre che le porte utilizzate in Administration Server siano disponibili.

3. Nel nuovo dispositivo installare il sistema di gestione database (DBMS) che verrà utilizzato da Administration Server.

   Quando si seleziona un DBMS, tenere in considerazione il numero di dispositivi coperti da Administration Server.

4. Installare Administration Server nel nuovo dispositivo.

   Se si sposta il server del database nel nuovo 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). 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.

5. Al termine dell'installazione ripristinare i dati di Administration Server nel nuovo dispositivo utilizzando l'utilità klbackup.

   > Se si utilizza SQL Server come DBMS nei dispositivi precedenti e nuovi, tenere presente che la versione di SQL Server installata nel nuovo dispositivo deve essere uguale o successiva alla versione di SQL Server installata nel dispositivo precedente. In caso contrario non è possibile recuperare i dati di Administration Server nel nuovo dispositivo.

6. Aprire Kaspersky Security Center 14 Web Console e connettersi ad Administration Server.

7. Verificare che tutti i dispositivi client siano collegati ad Administration Server.

8. Disinstallare Administration Server e il server del database dal dispositivo precedente.

Creazione di un Administration Server virtuale

È possibile creare Administration Server virtuali e aggiungerli ai gruppi di amministrazione.

Per creare e aggiungere un Administration Server virtuale:

1. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** ( ) accanto al nome dell'Administration Server desiderato.

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.

6. 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.

7. 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 14 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 14 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 14 Web Console.

  1. Nel dispositivo in cui è installato Kaspersky Security Center 14 Web Console, avviare il file di installazione ksc-web-console-<numero versione><numero build>.exe con un account con privilegi di amministratore.

2. Verrà avviata l'Installazione guidata.
3. Nella prima pagina dell'Installazione guidata selezionare l'opzione **Upgrade**.
4. Nella pagina **Tipo di modifica** selezionare l'opzione **Modifica impostazioni di connessione**.
5. Nella pagina **Administration Server attendibili** aggiungere l'Administration Server secondario desiderato.
6. Nell'ultima pagina della procedura guidata fare clic su **Modifica** per applicare le nuove impostazioni.
7. Al termine della riconfigurazione dell'applicazione, fare clic sul pulsante **Fine**.

- Utilizzare Kaspersky Security Center 14 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 14 Web Console.
- Utilizzare Administration Console basata su MMC per connettersi direttamente al server virtuale.

Gerarchia di Administration server

Un MSP può eseguire diversi Administration Server. Poiché può essere scomodo amministrare più Administration Server distinti, è possibile applicare una gerarchia.

In una gerarchia, Kaspersky Security Center Linux Administration Server può funzionare solo come server secondario gestito da un Administration Server primario di Kaspersky Security Center basato su Windows o Kaspersky Security Center Cloud Console.

Una configurazione "primario/secondario" per due Administration Server fornisce le seguenti opzioni:

- Un Administration Server secondario eredita i criteri e le attività 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.

Creazione di una gerarchia di Administration Server: l'aggiunta un Administration Server secondario

Espandi tutto | Comprimi tutto

In una gerarchia, Kaspersky Security Center Linux Administration Server può funzionare solo come server secondario gestito da un Administration Server primario di Kaspersky Security Center basato su Windows o Kaspersky Security Center Cloud Console.

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 14 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 **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 la Connessione guidata all'Administration Server secondario.
6. Nella prima pagina della procedura guidata compilare i seguenti campi:
   - Nome visualizzato dell'Administration Server secondario

     Nome con cui l'Administration Server secondario verrà visualizzato nella gerarchia. Facoltativamente è possibile immettere l'indirizzo IP come nome oppure 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.

- 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. Seguire le ulteriori istruzioni della procedura guidata.

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), è comunque possibile aggiungere un Administration Server secondario.

Per aggiungere come secondario un Administration Server non disponibile per la connessione tramite Kaspersky Security Center 14 Web Console:

1. Inviare il file del certificato del futuro Administration Server primario all'amministratore di sistema della sede 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 tramite 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 **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 secondario 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):

Nella finestra principale dell'applicazione fare clic sul nome di Administration Server, accanto all'icona **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 14 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 14 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 14 Web Console.

  1. Nel dispositivo in cui è installato Kaspersky Security Center 14 Web Console, avviare il file di installazione ksc-web-console-<numero versione><numero build>.exe con un account con privilegi di amministratore.
  2. Verrà avviata l'Installazione guidata.
  3. Nella prima pagina dell'Installazione guidata selezionare l'opzione **Upgrade**.
  4. Nella pagina **Tipo di modifica** selezionare l'opzione **Modifica impostazioni di connessione**.
  5. Nella pagina **Administration Server attendibili** aggiungere l'Administration Server secondario desiderato.
  6. Nell'ultima pagina della procedura guidata fare clic su **Modifica** per applicare le nuove impostazioni.
  7. Al termine della riconfigurazione dell'applicazione, fare clic sul pulsante **Fine**.

- Utilizzare Kaspersky Security Center 14 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 14 Web Console.
- Utilizzare Administration Console basata su MMC per connettersi direttamente al server virtuale.

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. Accedere a **UTENTI E RUOLI** → **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 verificare l'autorizzazione di modifica degli account utente** se si desidera richiedere le credenziali ogni volta che le impostazioni dell'account vengono modificate. In caso contrario, selezionare l'opzione **Consentire 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 14 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'applicazione di autenticazione nei propri dispositivi.

Passaggi

L'abilitazione della verifica in due passaggi per tutti gli utenti procede per fasi:

1. **Installazione di un'applicazione di autenticazione in un dispositivo**

   È possibile installare Google Authenticator, Microsoft Authenticator o qualsiasi altra applicazione di autenticazione che supporti l'algoritmo Time-based One-time Password.

2. **Sincronizzazione dell'ora dell'applicazione di autenticazione con l'ora del dispositivo in cui è installato Administration Server**

   Assicurarsi che l'ora impostata nell'applicazione di autenticazione sia sincronizzata con l'ora di Administration Server.

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. **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.

6. **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.

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 14 Web Console. Quando la verifica in due passaggi è abilitata per il proprio account, ogni volta che si accede a Kaspersky Security Center 14 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'applicazione 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'applicazione 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'applicazione di autenticazione. Se si modifica il nome dell'emittente del codice di sicurezza, è necessario emettere una nuova chiave segreta e passarla all'applicazione 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 applicazione di autenticazione, ad esempio Google Authenticator. Per generare il codice di sicurezza, è necessario sincronizzare l'ora impostata nell'applicazione di autenticazione con l'ora impostata per Administration Server.

Un'applicazione 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'applicazione di autenticazione.
3. L'applicazione di autenticazione genera un codice di sicurezza monouso che verrà specificato nella finestra di autenticazione di Administration Server.

È consigliabile installare un'applicazione di autenticazione in più di un dispositivo. Salvare la chiave segreta (o il codice QR) e conservarli in un luogo sicuro. Questo codice consentirà di ripristinare l'accesso a Kaspersky Security Center 14 Web Console nel caso in cui si perda l'accesso al dispositivo mobile.

Per proteggere l'utilizzo di Kaspersky Security Center, 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 14 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 14 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.

Se la verifica in due passaggi è abilitata per un account utente in Kaspersky Security Center Administration Server versione 13 o successive, l'utente non sarà in grado di accedere a Kaspersky Security Center Web Console versione 12, 12.1 o 12.2.

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'applicazione di autenticazione. Assicurarsi che l'ora impostata nell'applicazione 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. Accedere a **UTENTI E RUOLI** → **UTENTI**.
2. Fare clic sul nome dell'account.
3. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Protezione account**.
4. Nella scheda **Protezione account**:
   - Selezionare l'opzione **Richiedi nome utente, password e codice di sicurezza (verifica in due passaggi)** se si desidera abilitare la verifica in due passaggi per un account utente:
     - Nella finestra della verifica in due passaggi visualizzata immettere la chiave segreta nell'applicazione di autenticazione o eseguire la scansione del codice QR per ricevere il codice di sicurezza monouso.

       È possibile specificare manualmente la chiave segreta nell'applicazione di autenticazione o eseguire la scansione del codice QR tramite il dispositivo mobile.
     - 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**.
5. Fare clic sul pulsante **Salva**.

La verifica in due passaggi è stata abilitata per l'account.

Abilitazione della verifica in due passaggi 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. Se non è stata abilitata la verifica in due passaggi per il proprio account prima di abilitarla per tutti gli utenti, l'applicazione apre la finestra per abilitare la verifica in due passaggi per il proprio account.

Per abilitare la verifica in due passaggi per tutti gli utenti:

1. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** ( ) accanto al nome dell'Administration Server desiderato.

   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".

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 dell'account di un altro utente se l'account dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

Per disabilitare la verifica in due passaggi per un account utente:

1. Accedere a **UTENTI E RUOLI** → **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 **Protezione account**.
4. Nella scheda **Protezione account** 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.

Disabilitazione della verifica in due passaggi per tutti gli utenti

È possibile disabilitare la verifica in due passaggi 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. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** () accanto al nome dell'Administration Server desiderato.

   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.

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. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** () accanto al nome dell'Administration Server desiderato.

   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.

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. Accedere a **UTENTI E RUOLI** → **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 **Protezione account**.

4. Nella scheda **Protezione account** 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'applicazione 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'applicazione di autenticazione in un altro dispositivo mobile e generare una nuova chiave segreta per ripristinare l'accesso a Kaspersky Security Center 14 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'applicazione di autenticazione.

Per specificare un nuovo nome dell'emittente del codice di sicurezza:

1. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** ( ) accanto al nome dell'Administration Server desiderato.
   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Protezione account**.
3. Nella scheda **Protezione account** 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.

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.

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. Nella parte superiore dello schermo fare clic sull'icona **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.

Configurazione dell'interfaccia

È possibile configurare l'interfaccia di Kaspersky Security Center 14 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 14 Web Console in base al set di funzionalità utilizzate al momento:

1. Nella finestra principale dell'applicazione fare clic sul menu dell'account.
2. Nel menu a discesa selezionare **Opzioni di interfaccia**.
3. Nella finestra **Opzioni di interfaccia** visualizzata abilitare o disabilitare le opzioni desiderate.
4. Fare clic su **Salva**.

Successivamente, la console visualizza le sezioni nel menu principale in base alle opzioni abilitate. Se ad esempio si abilita **Mostra avvisi EDR**, nel menu principale viene visualizzata la sezione **MONITORAGGIO E GENERAZIONE DEI RAPPORTI → AVVISI**.

Individuazione dei dispositivi nella rete

Questa sezione descrive la ricerca e l'individuazione dei dispositivi nella rete.

Kaspersky Security Center 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 l'individuazione dispositivi 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. **Individuazione iniziale dispositivi**

   Dopo aver completato l'Avvio rapido guidato, eseguire manualmente l'individuazione dei dispositivi.

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.

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

Espandi tutto | Comprimi tutto

Kaspersky Security Center 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. 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 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 include automaticamente la rete 192.168.0.0/24 nell'elenco degli indirizzi di polling. Kaspersky Security Center 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 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. 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

Espandi tutto | Comprimi tutto

Inizialmente, Kaspersky Security Center 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 include automaticamente la rete 192.168.0.0/24 nell'elenco degli indirizzi di polling. Kaspersky Security Center 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 eseguirà il polling dell'intera rete.

Per aggiungere un nuovo intervallo IP:

1. 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**. Al termine del polling, è possibile visualizzare l'elenco dei dispositivi rilevati utilizzando il pulsante **Dispositivi**. 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. 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 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 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. Accedere a **INDIVIDUAZIONE E DISTRIBUZIONE → INDIVIDUAZIONE → INTERVALLI IP**.
2. Fare clic sul pulsante **Proprietà**.
3. Nella finestra visualizzata, attivare l'interruttore **Usa Zeroconf per il polling delle reti IPv6**.

Successivamente, Kaspersky Security Center inizia a eseguire il polling della rete. In questo caso gli intervalli IP specificati vengono ignorati.

Tag dispositivo

Questa sezione descrive i tag dispositivo e fornisce istruzioni per crearli e modificarli, nonché per l'assegnazione manuale o automatica di tag ai dispositivi.

Informazioni sui tag dispositivo

Kaspersky Security Center consente di eseguire il *tagging* dei dispositivi. Un tag è l'etichetta di un dispositivo 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. È possibile utilizzare il tagging manuale quando si desidera assegnare tag a un singolo dispositivo. Il tagging automatico viene eseguito da Kaspersky Security Center in base alle regole di tagging specificate.

Ai dispositivi viene assegnato automaticamente un tag 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 **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 **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

Per eliminare un tag dispositivo:

1. Nel menu principale accedere a **DISPOSITIVI → TAG → TAG DISPOSITIVO**.
2. Nell'elenco selezionare il pulsante di opzione accanto al tag dispositivo da 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.

> Il tag eliminato non viene rimosso automaticamente dalle regole di tagging automatico. Una volta eliminato, il tag verrà assegnato a un nuovo dispositivo solo quando il dispositivo soddisfa per la prima volta le condizioni di una regola per l'assegnazione del tag.

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 **DISPOSITIVI → TAG → TAG DISPOSITIVO**.
2. Fare clic sul collegamento **Visualizza dispositivi** accanto al tag per cui si desidera visualizzare i dispositivi assegnati.
   Se non viene visualizzato il collegamento **Visualizza dispositivi** accanto a un tag, il tag non è assegnato ad alcun dispositivo.

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 **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.

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.

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. Visualizzare i tag assegnati al dispositivo da cui si desidera rimuovere un tag.
2. Selezionare la casella di controllo accanto al tag da rimuovere.
3. Fare clic sul pulsante **Annulla assegnazione tag**.
4. 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.

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 **DISPOSITIVI → TAG → REGOLE DI TAGGING AUTOMATICO**.
- Nel menu principale accedere a **DISPOSITIVI → TAG**, 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.
   - **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.

Tag applicazione

Questa sezione descrive i tag applicazione e fornisce istruzioni per crearli e modificarli, nonché per l'assegnazione di tag alle applicazioni di terze parti.

Informazioni sui tag applicazione

Kaspersky Security Center Linux consente di assegnare tag alle applicazioni di terze parti (applicazioni realizzate da fornitori di software diversi da Kaspersky). 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. Selezionare la 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. Selezionare la 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.

Distribuzione delle applicazioni Kaspersky

In questa sezione viene descritta la distribuzione delle applicazioni Kaspersky nei dispositivi client dell'organizzazione tramite Kaspersky Security Center 14 Web Console.

Scenario: Distribuzione delle applicazioni Kaspersky

In questo scenario viene descritto come distribuire le applicazioni Kaspersky tramite Kaspersky Security Center 14 Web Console. È possibile utilizzare l'Avvio rapido guidato e la Distribuzione guidata della protezione oppure completare manualmente tutti i passaggi necessari.

La distribuzione delle applicazioni Kaspersky prevede diversi passaggi:

1. **Download del plug-in Web di gestione per l'applicazione**

   Scaricare il plug-in Web di gestione per Kaspersky Endpoint Security for Linux dal sito Web di Kaspersky, quindi aggiungere il plug-in a Kaspersky Security Center 14 Web Console.

2. **Download e creazione del pacchetto di installazione per Network Agent**

   Scaricare il pacchetto di distribuzione di Network Agent dal sito Web di Kaspersky, quindi creare un pacchetto di installazione di Network Agent.

   È possibile utilizzare il pacchetto di distribuzione scaricato per installare Network Agent in locale. A tale scopo, seguire le istruzioni fornite nella documentazione relativa a Kaspersky Endpoint Security for Linux.

3. **Download e creazione del pacchetto di installazione per Kaspersky Endpoint Security for Linux**

   Scaricare il pacchetto di distribuzione di Kaspersky Endpoint Security for Linux dal sito Web di Kaspersky, quindi creare un pacchetto di installazione di Kaspersky Endpoint Security for Linux.

4. **Creazione di pacchetti di installazione indipendenti (facoltativo)**

   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, è possibile ignorare i passaggi 5 e 6 indicati di seguito.

5. **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.

6. **Creazione e configurazione delle attività**

   È necessario configurare l'attività *Aggiornamento* di Kaspersky Endpoint Security for Linux.

   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 per l'attività è impostato su **Manualmente**, ma potrebbe essere preferibile scegliere un'altra opzione.

7. **Creazione dei criteri**

   Creare il criterio per Kaspersky Endpoint Security for Linux 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.

8. **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, è necessario aggiungere e installare il plug-in Web di gestione per l'applicazione.

Per aggiungere e installare un plug-in Web di gestione per un'applicazione Kaspersky:

1. Scaricare il plug-in Web di gestione per Kaspersky Endpoint Security for Linux dal sito Web di Kaspersky.
2. Aprire Kaspersky Security Center 14 Web Console.
3. Nell'elenco a discesa **Impostazioni della console** selezionare **Plug-in Web**.
   Verrà visualizzato un elenco dei plug-in di gestione disponibili.
4. Fare clic sul pulsante **Aggiungi da file**.
   Verrà visualizzata la finestra **Aggiungi da file**.
5. Fare clic sul pulsante **Carica file ZIP**.
6. Specificare il file ZIP scaricato del plug-in Web.
7. Fare clic sul pulsante **Carica firma**.
8. Specificare il file TXT scaricato della firma del plug-in Web.
9. Fare clic sul pulsante **Aggiungi**.
   Kaspersky Security Center verifica i file caricati, quindi aggiunge e installa il plug-in Web.
10. Al termine dell'installazione, fare clic su **OK**.

Il plug-in Web di gestione verrà installato con la configurazione predefinita e visualizzato nell'elenco dei plug-in Web di gestione.

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.
- 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:
   - Accedere a **INDIVIDUAZIONE E DISTRIBUZIONE → DISTRIBUZIONE E ASSEGNAZIONE → PACCHETTI DI INSTALLAZIONE**.
   - 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. Nella prima pagina della procedura guidata selezionare **Crea pacchetto di installazione da un file**.
4. Nella pagina successiva della procedura guidata 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. Nella pagina successiva della procedura guidata 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 (Installer.exe) 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 terze parti. Per creare un pacchetto di installazione indipendente per un'applicazione di terze parti, 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:

   - Accedere a **INDIVIDUAZIONE E DISTRIBUZIONE → DISTRIBUZIONE E ASSEGNAZIONE → PACCHETTI DI INSTALLAZIONE**.
   - 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. Nella prima pagina della procedura guidata assicurarsi che l'opzione **Installa Network Agent con questa applicazione** sia abilitata, 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. Nella pagina **Spostare nell'elenco dei dispositivi gestiti** della procedura guidata 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. Nella pagina successiva della procedura guidata, al termine del processo di creazione del pacchetto di installazione indipendente, fare clic sul pulsante **FINE**.

   La Creazione guidata pacchetto di installazione indipendente si chiude.

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.

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 vengono visualizzate le seguenti proprietà:

- **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:

- 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**.

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 ai dispositivi più in modo facile e rapido, è possibile specificare i dispositivi nella finestra della procedura guidata in uno dei seguenti modi:

- **Selezionare i dispositivi della rete rilevati da Administration Server**. In questo caso l'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i 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.
- **Assegnare 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.
- **Assegnare un'attività a un gruppo di amministrazione**. In questo caso l'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione creato precedentemente.

Per una corretta installazione remota in un dispositivo in cui Network Agent non è stato installato, è necessario che le seguenti porte siano aperte: a) TCP 139 e 445; b) UDP 137 e 138. Per impostazione predefinita, queste porte sono aperte in tutti i dispositivi inclusi nel dominio. Sono aperte automaticamente utilizzando l'utilità di preparazione dell'installazione remota.

Installazione di un'applicazione in dispositivi specifici

Espandi tutto | Comprimi tutto

Questa sezione contiene informazioni su come installare un'applicazione in remoto in un gruppo di amministrazione, in dispositivi con indirizzi IP specifici o in una selezione di dispositivi gestiti.

Per installare un'applicazione in dispositivi specifici:

1. Stabilire una connessione all'Administration Server che controlla i dispositivi desiderati.

2. Nel menu principale accedere a **DISPOSITIVI → ATTIVITÀ**.

3. Fare clic su **Aggiungi**.

   Verrà avviata l'Aggiunta guidata attività.

4. Nel campo **Tipo di attività** selezionare **Installa l'applicazione in remoto**.

5. 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.

   - **Usa indirizzi dei dispositivi specificati manualmente o importati 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. Seguire le istruzioni della procedura guidata.

   Verrà creata un'attività per l'installazione remota dell'applicazione selezionata nella procedura guidata nei dispositivi specificati. Se è stata selezionata l'opzione **Assegna attività a un gruppo di amministrazione**, si tratta di un'attività di gruppo.

7. 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 nei dispositivi specificati.

Installazione di un'applicazione utilizzando i criteri di gruppo di Active Directory

Kaspersky Security Center consente di installare le applicazioni Kaspersky nei dispositivi gestiti utilizzando i criteri di gruppo di Active Directory.

È possibile installare le applicazioni tramite i criteri di gruppo di Active Directory solo da pacchetti di installazione che includono Network Agent.

Per installare un'applicazione utilizzando i criteri di gruppo di Active Directory:

1. Eseguire la Distribuzione guidata della protezione. Seguire le istruzioni della procedura guidata.

2. Nella pagina **Impostazioni dell'attività di installazione remota** della Distribuzione guidata della protezione abilitare l'opzione **Assegna l'installazione del pacchetto in Criteri di gruppo di Active Directory**.

3. Nella pagina **Selezionare gli account per l'accesso ai dispositivi** selezionare l'opzione **Account richiesto (Network Agent non utilizzato)**.

4. Aggiungere l'account con privilegi di amministratore nel dispositivo in cui è installato Kaspersky Security Center o l'account incluso nel gruppo di dominio Proprietari autori criteri di gruppo.

5. Concedere le autorizzazioni all'account selezionato:

   a. Accedere a **Pannello di controllo → Strumenti di amministrazione** e aprire **Gestione Criteri di gruppo**.

   b. Fare clic sul nodo con il dominio desiderato.

   c. Fare clic sulla sezione **Delega**.

   d. Nell'elenco a discesa **Autorizzazione** selezionare **Collega oggetti Criteri di gruppo**.

   e. Fare clic su **Aggiungi**.

   f. Nella finestra **Seleziona utente, computer o gruppo** visualizzata selezionare l'account necessario.

g. Fare clic su **OK** per chiudere la finestra **Seleziona utente, computer o gruppo**.

h. Nell'elenco **Gruppi e utenti** selezionare l'account appena aggiunto, quindi fare clic su **Avanzate** → **Avanzate**.

i. Nell'elenco **Autorizzazioni** fare doppio clic sull'account appena aggiunto.

j. Concedere le seguenti autorizzazioni:

- **Creare oggetti Criteri di gruppo**
- **Eliminare oggetti Criteri di gruppo**
- **Creare oggetti del contenitore Criteri di gruppo**
- **Eliminare oggetti dal contenitore Criteri di gruppo**

k. Fare clic su **OK** per salvare le modifiche.

6. Definire altre impostazioni seguendo le istruzioni della procedura guidata.
7. Eseguire l'attività di installazione remota creata manualmente o attenderne l'avvio pianificato.

Verrà avviata la seguente sequenza di installazione remota:

1. Durante l'esecuzione dell'attività, verranno creati i seguenti oggetti nel dominio che include i dispositivi client per il set specificato:
   - Oggetto Criteri di gruppo denominato **Kaspersky_AK{GUID}**.
   - Un gruppo di protezione che corrisponde all'oggetto Criteri di gruppo. Questo gruppo di protezione include i dispositivi client coperti dall'attività. Il contenuto del gruppo di protezione definisce l'ambito dell'oggetto Criteri di gruppo.
2. Kaspersky Security Center installa le applicazioni Kaspersky selezionate nei dispositivi client direttamente da Share, ovvero la cartella di rete condivisa dell'applicazione. Nella cartella di installazione di Kaspersky Security Center verrà creata una cartella nidificata ausiliaria che contiene il file .msi per l'applicazione da installare.
3. Quando si aggiungono nuovi dispositivi all'ambito dell'attività, questi vengono aggiunti al gruppo di protezione al successivo avvio dell'attività. Se nella pianificazione dell'attività è selezionata l'opzione **Esegui attività non effettuate**, i dispositivi vengono aggiunti al gruppo di protezione immediatamente.
4. Quando si eliminano dispositivi dall'ambito dell'attività, questi vengono eliminati dal gruppo di protezione al successivo avvio dell'attività.
5. Quando si elimina un'attività da Active Directory, vengono eliminati anche l'oggetto Criteri di gruppo, il collegamento all'oggetto Criteri di gruppo e il gruppo di protezione corrispondente.

Se si desidera applicare un altro schema di installazione tramite Active Directory, è possibile configurare manualmente le impostazioni richieste. Questa operazione può essere ad esempio necessaria nei seguenti casi:

- Quando l'amministratore della protezione anti-virus non dispone dei diritti necessari per apportare modifiche ad Active Directory per determinati domini
- Quando il pacchetto di installazione originale deve essere archiviato in una risorsa di rete distinta
- Quando è necessario collegare un oggetto Criteri di gruppo a specifiche unità Active Directory

Sono disponibili le seguenti opzioni per l'utilizzo di uno schema di installazione alternativo tramite Active Directory:

- Se è necessario eseguire l'installazione direttamente dalla cartella condivisa di Kaspersky Security Center, nelle proprietà dell'oggetto Criteri di gruppo specificare il file .msi presente nella sottocartella exec della cartella del pacchetto di installazione per l'applicazione desiderata.
- Se il pacchetto di installazione deve essere posizionato in un'altra risorsa di rete, copiare in tale risorsa l'intero contenuto della cartella exec, perché questa contiene, oltre al file con estensione .msi, i file di configurazione generati al momento della creazione del pacchetto. Per installare la chiave di licenza insieme all'applicazione, copiare anche il file chiave in questa cartella.

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**.

   Verrà creata 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

Espandi tutto | Comprimi tutto

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. Nel menu principale accedere a **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 14 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 14 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 14 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.

Sostituzione di applicazioni di protezione di terze parti

L'Installazione delle applicazioni di protezione Kaspersky tramite Kaspersky Security Center Linux può richiedere la rimozione di software di terze parti incompatibile con l'applicazione da installare. Kaspersky Security Center offre diversi modi di rimuovere le applicazioni di terze parti.

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 consente di rimuovere le applicazioni incompatibili prima di installare un'applicazione di protezione in un dispositivo gestito.

Istruzioni dettagliate: Rimozione delle applicazioni incompatibili prima dell'installazione

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.

Istruzioni dettagliate: Creazione di un'attività

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 **DISPOSITIVI** → **ATTIVITÀ**.
2. Fare clic su **Aggiungi**.
   Verrà avviata l'Aggiunta guidata attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Per l'applicazione Kaspersky Security Center, selezionare il tipo di attività **Disinstalla l'applicazione in remoto**.
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 i dispositivi a cui verrà assegnata l'attività.
6. 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 applicazione incompatibile**

     Viene visualizzato un elenco di applicazioni incompatibili con le applicazioni di protezione Kaspersky o Kaspersky Security Center. Selezionare le caselle di controllo accanto alle applicazioni da 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.

     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 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 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 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.

7. 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 invece 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 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 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 verifica se le impostazioni dell'utilità di disinstallazione sono applicabili al sistema operativo del dispositivo client. Se le impostazioni non sono applicabili, Kaspersky Security Center non trasmette i file e non tenta di disinstallare l'applicazione. Ad esempio, per disinstallare un'applicazione dai dispositivi di un gruppo di amministrazione che include dispositivi che eseguono vari sistemi operativi, è possibile assegnare l'attività di disinstallazione al gruppo di amministrazione e quindi abilitare questa opzione per ignorare i dispositivi che eseguono un sistema operativo diverso da quello desiderato.

8. 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).

   - **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.

9. 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)**

     Se questa opzione è selezionata, è possibile specificare l'account con cui verrà eseguito il programma di installazione dell'applicazione. È possibile specificare l'account utente se Network Agent non è stato installato nei dispositivi a cui è assegnata l'attività.

     È possibile specificare più account utente, ad esempio se nessuno di essi dispone di tutti i diritti richiesti per tutti i dispositivi a cui è assegnata l'attività. In questo caso, tutti gli account che sono stati aggiunti vengono utilizzati per l'esecuzione dell'attività, consecutivamente, dall'alto in basso.

     Se non è stato aggiunto alcun account, l'attività sarà eseguita tramite l'account con cui viene eseguito Administration Server.

10. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione 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.

11. Fare clic sul pulsante **Fine**.

    L'attività verrà creata e visualizzata nell'elenco delle attività.

12. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

13. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività.

14. Fare clic sul pulsante **Salva**.

15. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di disinstallazione remota, l'applicazione selezionata verrà rimossa dai dispositivi selezionati.

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.

Dopo aver preparato il dispositivo SUSE Linux Enterprise Server 15, distribuire e installare Network Agent.

Applicazioni Kaspersky: licensing e attivazione

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 aggiuntiva con uno dei metodi sopra elencati. Un'applicazione Kaspersky utilizza una chiave attiva al momento e memorizza una chiave aggiuntiva 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

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 accedere a **OPERAZIONI** → **LICENSING** → **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 14 Web Console consente di distribuire una chiave di licenza ai dispositivi client tramite l'attività di *distribuzione della chiave di licenza*.

Per distribuire una chiave di licenza ai dispositivi client:

1. Nel menu principale accedere a **DISPOSITIVI → ATTIVITÀ**.
2. Fare clic su **Aggiungi**.

   Verrà avviata l'Aggiunta guidata attività.
3. Selezionare l'applicazione per cui si desidera aggiungere una chiave di licenza.
4. Dall'elenco **Tipo di attività** selezionare **Aggiungi chiave di licenza**.
5. Seguire le istruzioni della procedura guidata.
6. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione 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.
7. Fare clic sul pulsante **Crea**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
8. Per eseguire l'attività, selezionarla nell'elenco delle attività e fare clic sul pulsante **Avvia**.

Quando l'attività viene eseguita, 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.

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 distribuire manualmente una chiave di licenza in un secondo momento.

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 **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**, quindi aprire la sezione **Licenza**.

Verranno visualizzate le informazioni principali sulla chiave di licenza attiva e quella aggiuntiva.

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.

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. Accedere a **OPERAZIONI** → **LICENSING** → **LICENZE DI KASPERSKY**.
2. Selezionare il file chiave o il codice di attivazione che si desidera eliminare dall'archivio.
3. Fare clic sul pulsante **Elimina**.
4. Confermare l'operazione facendo clic sul pulsante **OK**.

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 dei Contratti di licenza con l'utente finale 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 accedere a **MONITORAGGIO E GENERAZIONE DEI RAPPORTI → DASHBOARD**, quindi fare clic sul collegamento **Visualizza licenze in scadenza** accanto alla 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: 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 14 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 14 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 della protezione di rete

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 dall'organizzazione. Pertanto, è consigliabile ottimizzare tali criteri e attività e creare altri criteri e attività, se necessario per la rete.

Prerequisiti

Prima di iniziare, verificare di avere:

- Installato Kaspersky Security Center Administration Server
- Installato Kaspersky Security Center 14 Web Console
- completato lo scenario di installazione principale di Kaspersky Security Center
- 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

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 anche 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 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 gli incidenti 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 Administration Server e Kaspersky Security Center 14 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 crea il criterio predefinito per Kaspersky Endpoint Security for Linux. 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, Kaspersky Security Center 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 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 Administration Server e Kaspersky Security Center 14 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 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 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 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.

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.

Impostazioni del criterio di Network Agent

Espandi tutto | Comprimi tutto

Per configurare il criterio di Network Agent:

1. Nel menu principale accedere a **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.

Generale

In questa scheda è possibile modificare lo stato del criterio e specificare l'ereditarietà delle impostazioni criterio:

- Nella sezione **Stato criterio** è possibile selezionare una 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 gruppi di amministrazione nidificati, ovvero ai criteri figlio.
    - Nel gruppo **Ereditarietà impostazioni** della sezione **Generale** nella finestra delle proprietà di ogni criterio figlio, l'opzione **Eredita impostazioni dal criterio padre** sarà abilitata automaticamente.

    Se questa opzione è abilitata, le impostazioni dei criteri figlio 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 vengono distribuiti in base al livello di importanza nelle seguenti sezioni nella scheda **Configurazione eventi**:

- **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.

Nella sezione **Avviso** è ad esempio possibile configurare il tipo di evento **Si è verificato un incidente**. 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 incidente**, 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 incidente, è possibile gestire tale incidente utilizzando le impostazioni di un dispositivo gestito.

Impostazioni applicazione

Impostazioni

Nella sezione **Impostazioni** è possibile configurare il criterio di Network Agent:

- **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 o fuori sede al momento della distribuzione del criterio al dispositivo gestito
  - 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 criterio attivi

    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.

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.

Rete

La sezione **Rete** include tre sottosezioni:

- **Connettività**
- **Profili connessione**
- **Pianificazione connessione**

Nella sottosezione **Connettività** 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.

  - 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 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. La porta UDP predefinita per la connessione al server proxy KSN è la 15111.

- 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** della sezione **Rete** è possibile specificare le impostazioni del percorso di rete e abilitare la modalità fuori sede quando Administration Server non è disponibile. Le impostazioni nella sezione **Profili connessione** sono disponibili solo nei dispositivi che eseguono Windows:

- 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. Si consiglia di non utilizzare questa opzione.

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

Nel gruppo di impostazioni **Profili connessione** non è possibile aggiungere nuovi elementi all'elenco **Profili connessione di Administration Server**, pertanto il pulsante **Aggiungi** è inattivo. Non è neanche possibile modificare i profili di connessione preimpostati.

- **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 degli intervalli 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, Administration Server esegue automaticamente il polling degli intervalli IP in base alla pianificazione configurata facendo clic sul collegamento **Imposta pianificazione di polling**.

  Se questa opzione è disabilitata, Administration Server non esegue il polling degli intervalli IP.

  La frequenza di polling degli intervalli 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.

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 abilitata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.
  Per impostazione predefinita, questa casella di controllo è disabilitata.

- **Nome utente**
- **Password**

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.

Cronologia revisioni

In questa scheda è possibile visualizzare l'elenco delle revisioni del criterio ed eseguire il rollback delle modifiche apportate al criterio, se necessario.

Modifica della priorità per le regole di spostamento dei dispositivi

Tutte le regole di spostamento dei dispositivi hanno priorità.

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.

Attività

Questa sezione descrive le attività utilizzate da Kaspersky Security Center.

Informazioni sulle attività

Kaspersky Security Center 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 14 Web Console solo se il plug-in di gestione per tale applicazione è installato in Kaspersky Security Center 14 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 14 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. Nel menu principale accedere a **DISPOSITIVI** → **ATTIVITÀ**.
2. Fare clic su **Aggiungi**.

   Verrà avviata l'Aggiunta guidata 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 **Completare la creazione 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.

4. Fare clic sul pulsante **Fine**.

L'attività verrà creata e visualizzata nell'elenco delle attività.

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.

Per avviare un'attività manualmente:

1. Nel menu principale accedere a **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,

Accedere a **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 for Linux.

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

Espandi tutto | Comprimi tutto

Questa sezione elenca le impostazioni che è possibile visualizzare e specificare per le attività.

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:
  - Avvio pianificato

    Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

    - 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 lunedì 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 abilitata.

- 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 18:00:00.

- 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.

- 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, vengono eseguite solo le attività pianificate nei dispositivi client. Per le opzioni **Manualmente**, **Una sola volta** e **Immediatamente**, le attività sono 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 abilitata.

- 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 dell'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.

- **Assegna 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.

- **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.

- 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:

  - Attiva il dispositivo prima dell'avvio dell'attività tramite Wake-on-LAN (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 il dispositivo 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 l'attività se è in esecuzione da 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:

  - Sezione **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.**

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. Nella scheda **DISPOSITIVI** selezionare **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

Espandi tutto | Comprimi tutto

Specificare le nuove credenziali attualmente valide nel sistema. Quando si passa al passaggio successivo della procedura guidata, Kaspersky Security Center 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 14 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 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**.

Gestione dei dispositivi client

Questa sezione descrive come gestire i dispositivi nei gruppi di amministrazione.

Impostazioni di un dispositivo gestito

Espandi tutto | Comprimi tutto

Per visualizzare le impostazioni di un dispositivo gestito:

1. Selezionare **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.

Generale

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.

- **Gruppo**

  Gruppo di amministrazione che include il dispositivo client.

- **Ultimo aggiornamento**

  Data dell'ultimo aggiornamento dei database o delle applicazioni.

- **Ultima visibilità**

  Data e ora in cui il dispositivo è risultato visibile nella rete per l'ultima volta.

- **Connesso ad Administration Server**

  Data e ora dell'ultima connessione del Network Agent installato nel dispositivo client ad Administration Server.

- **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.

Rete

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.

Sistema

La sezione **Sistema** fornisce le informazioni sul sistema operativo installato nel dispositivo client.

Protezione

Nella sezione **Protezione** vengono visualizzate informazioni sullo stato corrente della protezione anti-virus nel 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.

- Tutti i problemi

  Questa tabella contiene un elenco completo dei problemi rilevati dalle applicazioni gestite installate nel dispositivo client. Ogni problema è accompagnato da uno stato, che l'applicazione suggerisce di assegnare al dispositivo per il problema.

- Protezione in tempo reale

  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 su richiesta

  Data e ora dell'ultima scansione virus eseguita nel dispositivo client.

- Numero totale di minacce rilevate

  Numero totale di minacce rilevate nel dispositivo client dall'installazione dell'applicazione anti-virus (prima scansione) o dall'ultimo azzeramento del contatore delle minacce.

- Minacce attive

  Numero di file non elaborati nel dispositivo client.

  Questo campo ignora il numero di file non elaborati nei dispositivi mobili.

Stato dispositivo definito dall'applicazione

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

Nella sezione **Applicazioni** sono elencate tutte le applicazioni Kaspersky installate nel dispositivo client. È 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

La sezione **Criteri attivi e profili criterio** elenca i criteri e i profili criterio attualmente attivi nel dispositivo gestito.

Attività

Nella sezione **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 connessione non viene stabilita, lo stato non viene visualizzato.

Eventi

Nella sezione **Eventi** sono visualizzati gli eventi registrati in Administration Server per il dispositivo client selezionato.

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.

File eseguibili

La sezione **File eseguibili** visualizza 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

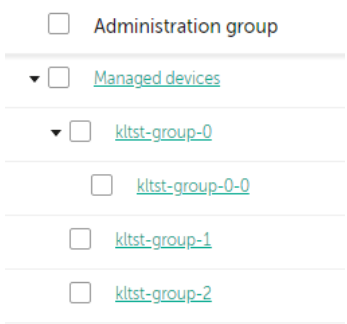
  Fare clic sul pulsante **Proprietà** per visualizzare e configurare il punto di distribuzione con cui interagisce il dispositivo.

Registro hardware

Nella sezione **Registro hardware** è possibile visualizzare le informazioni relative all'hardware installato nel dispositivo client.

Creazione di 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).



Per creare un gruppo di amministrazione:

1. Accedere a **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. Accedere a **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.

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 **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.

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 e così via.

Creazione delle regole di spostamento dei dispositivi

Espandi tutto | Comprimi tutto

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, passare alla scheda **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.

- **Applica regola**

  È possibile selezionare una delle seguenti opzioni:

  - Eseguire una volta per ogni dispositivo.

    La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri.

  - Eseguire una volta per ogni 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.

  - Regola applicata continuamente.

    La regola viene applicata in base alla pianificazione impostata automaticamente da Administration Server (in genere, con una frequenza di alcune ore).

- **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.

- **Abilita regola**

  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.

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. 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. Nel menu principale, passare alla scheda **DISPOSITIVI → REGOLE DI SPOSTAMENTO**.

   È inoltre possibile selezionare **INDIVIDUAZIONE E DISTRIBUZIONE → DISTRIBUZIONE E ASSEGNAZIONE** e quindi selezionare **REGOLE DI SPOSTAMENTO** nel menu.

   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.

   - **Applica regola**

     È possibile selezionare una delle seguenti opzioni:

     - Eseguire una volta per ogni dispositivo.

       La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri.

     - Eseguire una volta per ogni 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.

     - Regola applicata continuamente.

       La regola viene applicata in base alla pianificazione impostata automaticamente da Administration Server (in genere, con una frequenza di alcune ore).

   - **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.

   - **Abilita regola**

     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.

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

Espandi tutto | Comprimi tutto

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.

- **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 14 Network Agent** o **Kaspersky Security Center 14 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, passare alla sezione **DISPOSITIVI** → **DISPOSITIVI GESTITI**.
  2. Fare clic sul pulsante **Impostazioni colonne** ( ) sulla 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.

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. Accedere a **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 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.

Per spostare uno o più dispositivi 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, passare a **DISPOSITIVI** → **Gruppi** → **<nome gruppo>** → **DISPOSITIVI GESTITI**.
   - Per aprire il gruppo **DISPOSITIVI NON ASSEGNATI**, passare a **INDIVIDUAZIONE E DISTRIBUZIONE** → **DISPOSITIVI NON ASSEGNATI**.
2. Selezionare le caselle di controllo accanto ai dispositivi che si desidera spostare in un gruppo differente.
3. Fare clic sul pulsante **Sposta nel gruppo**.
4. Nella gerarchia dei gruppi di amministrazione selezionare la casella di controllo accanto al gruppo di amministrazione in cui si desidera spostare i dispositivi selezionati.
5. Fare clic sul pulsante **Sposta**.

I dispositivi selezionati verranno spostati nel gruppo di amministrazione selezionato.

Modifica di Administration Server per i dispositivi client

Espandi tutto | Comprimi tutto

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 l'Aggiunta guidata attività. Seguire le istruzioni della procedura guidata. Nella finestra **Nuova attività** dell'Aggiunta guidata attività, selezionare l'applicazione **Kaspersky Security Center 14** 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.

- Usa indirizzi dei dispositivi specificati manualmente o importati 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.

Visualizzazione e configurazione delle azioni per i dispositivi inattivi

Espandi tutto | Comprimi tutto

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 **DISPOSITIVI** → **GERARCHIA DEI GRUPPI**.
2. Fare clic sul nome del gruppo di amministrazione desiderato.

   Verrà visualizzata la finestra delle proprietà del 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.

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 virus, 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 virus non eseguita da molto tempo	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma l'attività Scansione virus non viene eseguita 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.
Incidenti non elaborati rilevati	Sono stati rilevati nel dispositivo alcuni incidenti non elaborati. Gli incidenti 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 l'individuazione dispositivi, 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.	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. Aprire la finestra delle proprietà in uno dei seguenti modi:
   - Nella cartella **Criteri** nel menu di scelta rapida di un criterio di Administration Server selezionare **Proprietà**.

- Selezionare **Proprietà** nel menu di scelta rapida di un gruppo di amministrazione.

2. Nella finestra delle proprietà visualizzata, nel riquadro **Sezioni**, selezionare **Stato dispositivo**.
3. Nel riquadro a destra, nella sezione **Imposta su Critico se è specificato** , selezionare la casella di controllo accanto a una condizione nell'elenco.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio padre.

4. Impostare il valore richiesto per la condizione selezionata.
   È possibile impostare i valori per alcune condizioni, ma non per tutte.
5. 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. Aprire la finestra delle proprietà in uno dei seguenti modi:
   - Nella cartella **Criteri** nel menu di scelta rapida del criterio di Administration Server selezionare **Proprietà**.
   - Selezionare **Proprietà** nel menu di scelta rapida del gruppo di amministrazione.
2. Nella finestra delle proprietà visualizzata, nel riquadro **Sezioni**, selezionare **Stato dispositivo**.
3. Nel riquadro a destra, nella sezione **Imposta su Avviso se è specificato** selezionare la casella di controllo accanto a una condizione nell'elenco.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio padre.

4. Impostare il valore richiesto per la condizione selezionata.
   È possibile impostare i valori per alcune condizioni, ma non per tutte.
5. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Avviso*.

Criteri e profili criterio

In Kaspersky Security Center 14 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 figlio.

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
Undefined	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*.
Enforce	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:

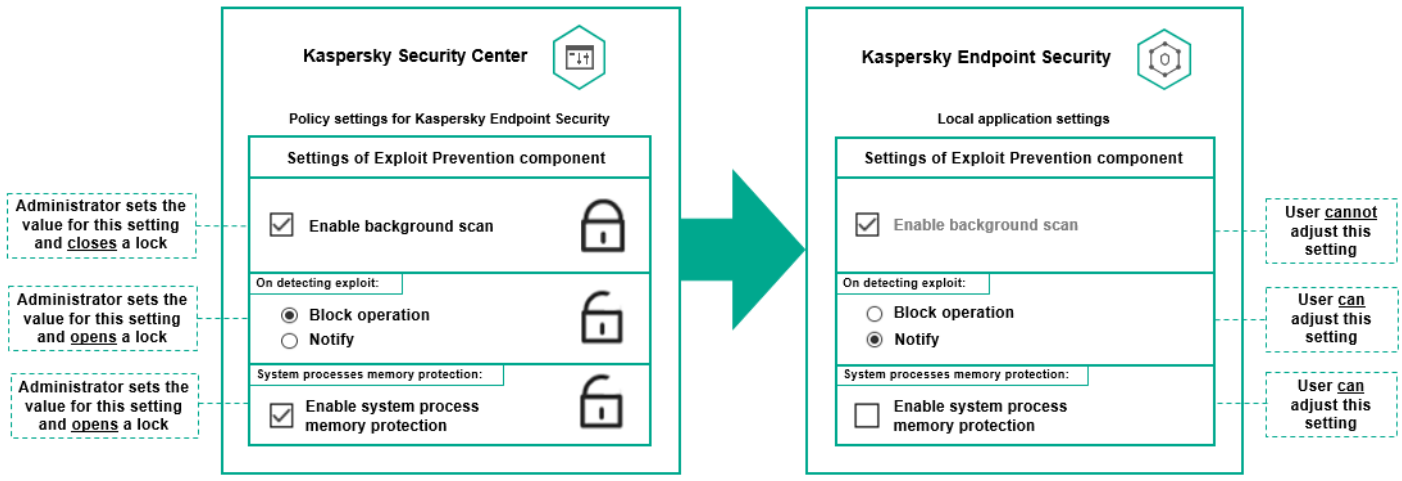
- Blocco delle impostazioni per il criterio di un sottogruppo di amministrazione
- Blocco delle impostazioni di un'applicazione Kaspersky in un dispositivo gestito

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 locale 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 di criteri

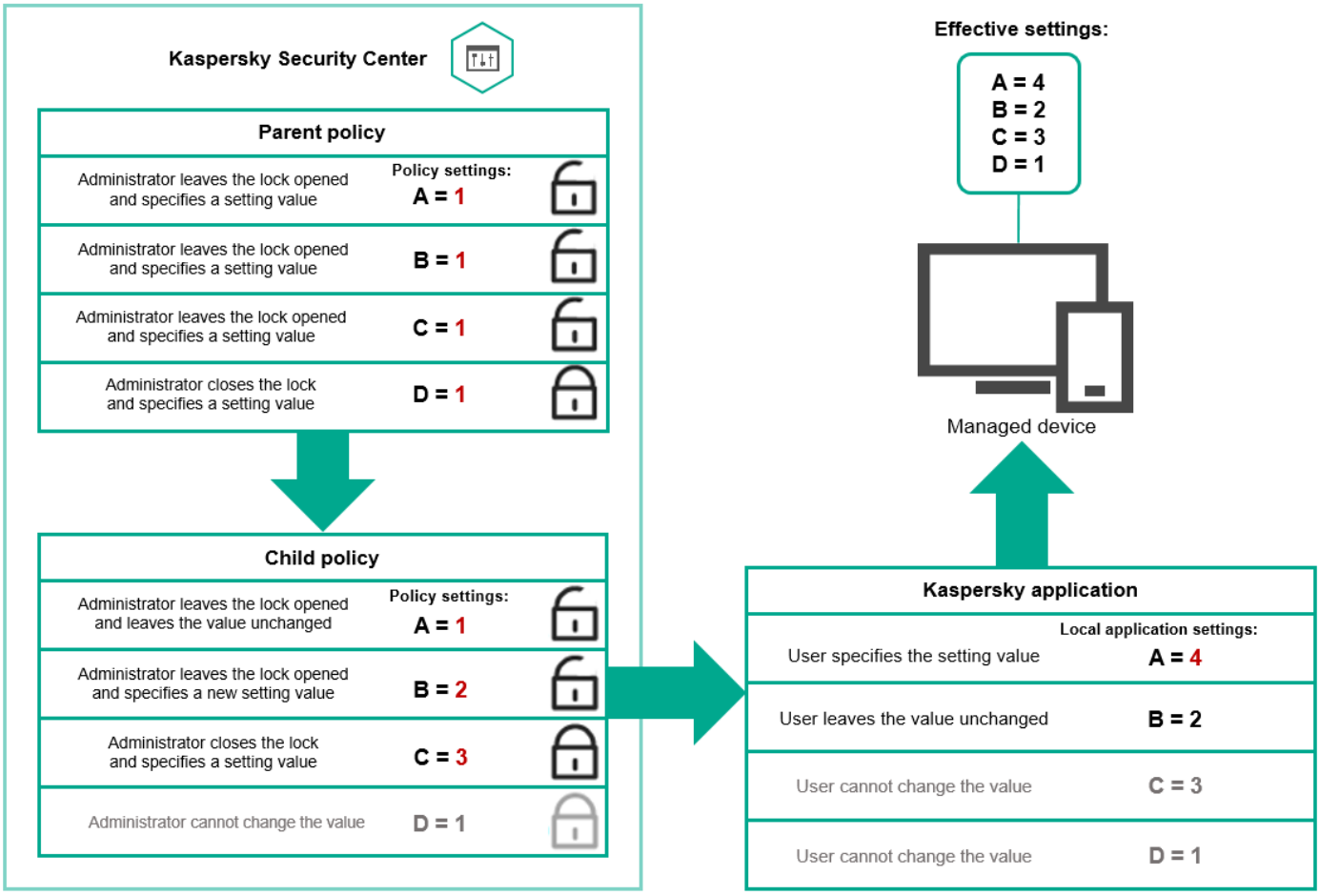
Se dispositivi diversi richiedono impostazioni diverse, è possibile organizzare i dispositivi in gruppi di amministrazione.

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 figlio) di un criterio di un gruppo di amministrazione (padre) di livello superiore.

Da questo momento in poi, un criterio per un gruppo padre viene denominato anche *criterio padre*. Un criterio per un sottogruppo (gruppo figlio) viene inoltre denominato *criterio figlio*.

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).

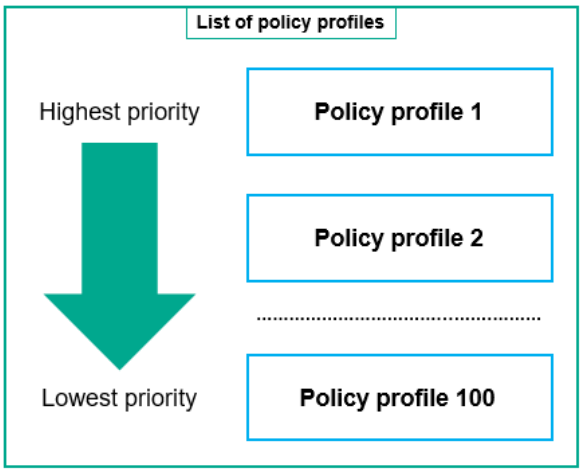


Gerarchia di criteri

Profili criterio in una gerarchia di criteri

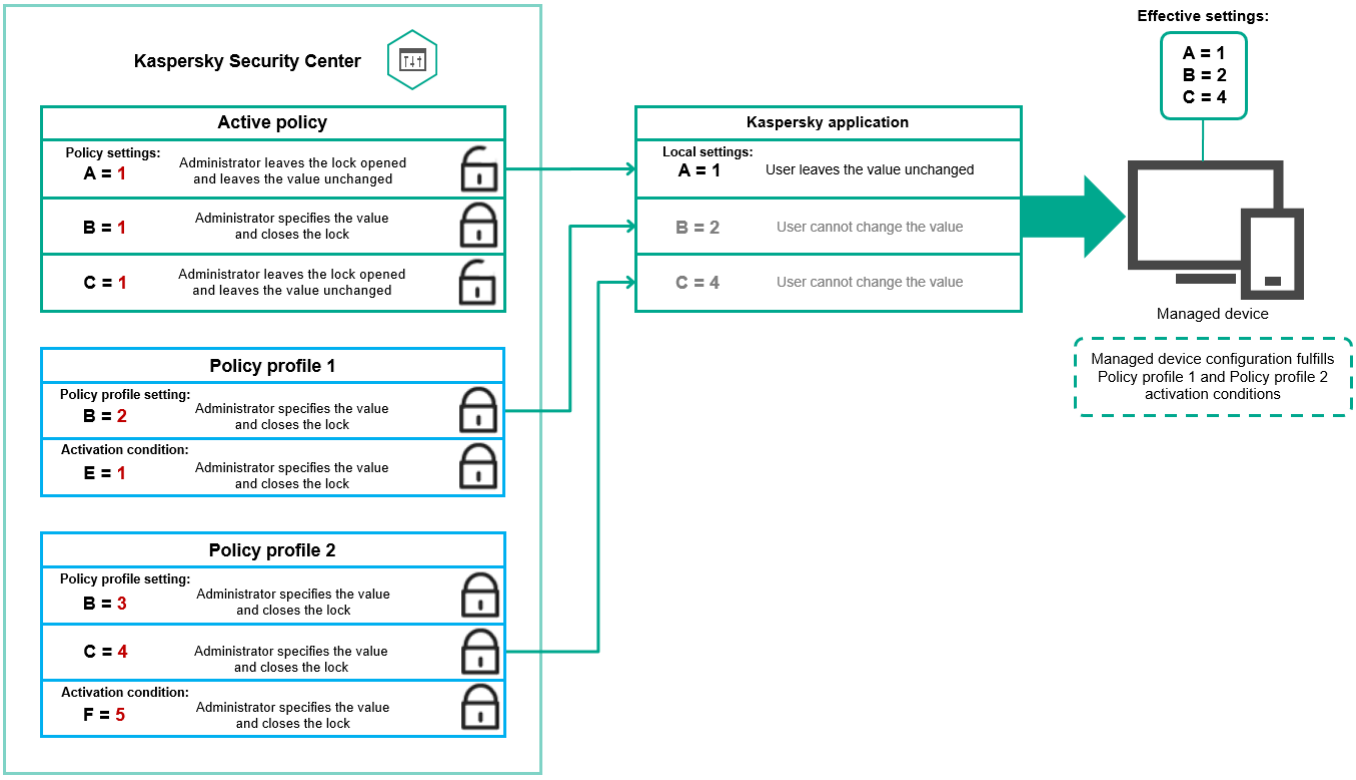
I profili criterio hanno le seguenti condizioni di assegnazione della priorità:

- 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).

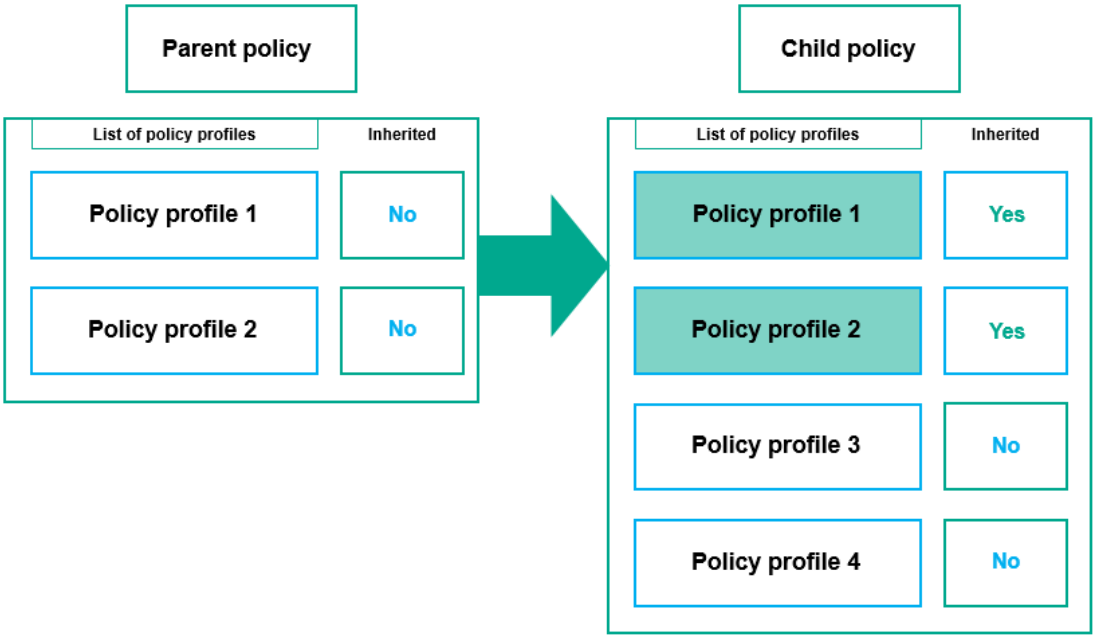


La configurazione del dispositivo gestito soddisfa le condizioni di attivazione di diversi profili criterio

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).

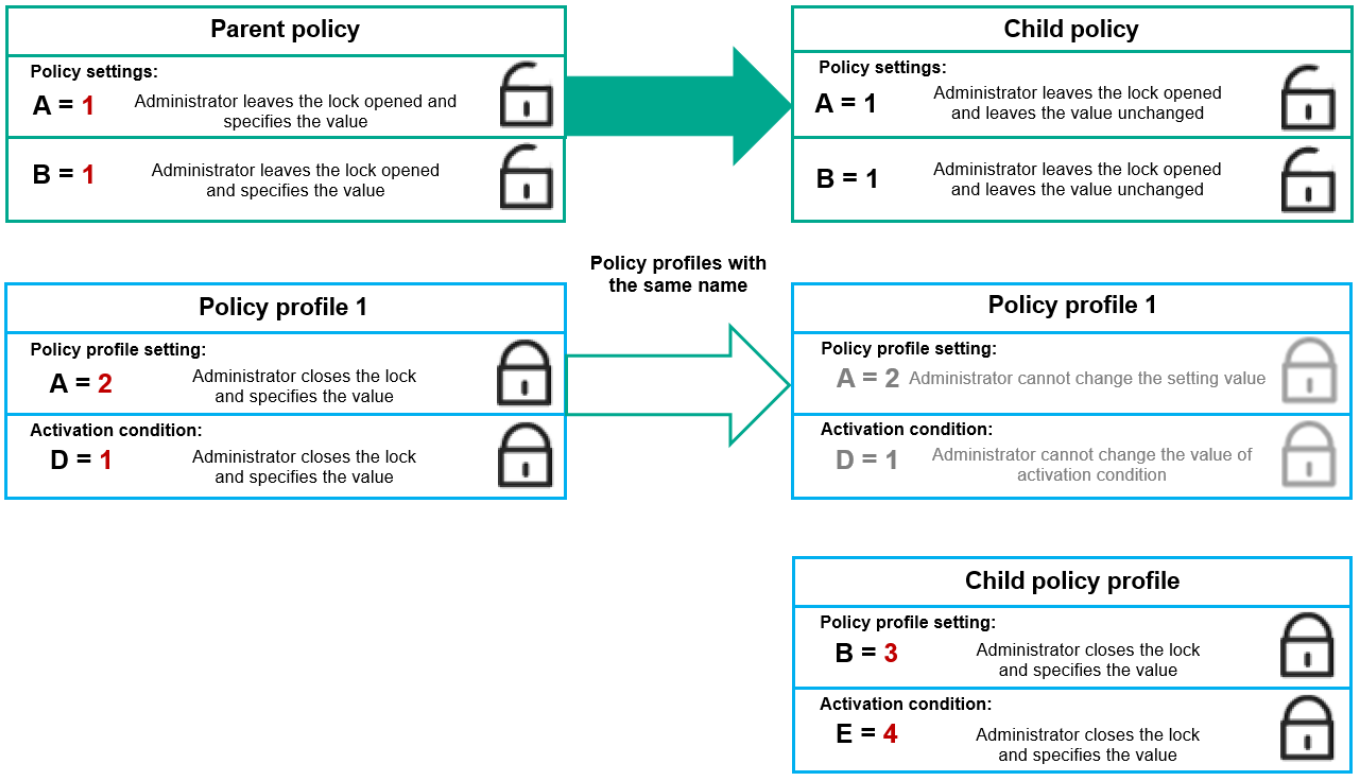


Ereditarietà dei profili criterio

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 padre

- 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 **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 profilo:

1. Accedere a **DISPOSITIVI** → **CRITERI E PROFILI**.
2. Fare clic su **Aggiungi**.

   Verrà aperta la finestra **Selezionare l'applicazione**.
3. Selezionare l'applicazione per cui si desidera creare un criterio.
4. Fare clic su **Avanti**.

   Verrà visualizzata la finestra delle impostazioni del nuovo criterio, con la scheda **Generale** selezionata.
5. Se si desidera, modificare il nome predefinito, lo stato predefinito e le impostazioni di ereditarietà predefinite del criterio.
6. 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.
7. 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

   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.
8. Fare clic su **Salva** per salvare il criterio.

Il criterio verrà visualizzato nell'elenco dei criteri.

Impostazioni generali dei criteri

Espandi tutto | Comprimi tutto

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 gruppi di amministrazione nidificati, ovvero ai criteri figlio.
    - Nel gruppo **Ereditarietà impostazioni** della sezione **Generale** nella finestra delle proprietà di ogni criterio figlio, l'opzione **Eredita impostazioni dal criterio padre** sarà abilitata automaticamente.

    Se questa opzione è abilitata, le impostazioni dei criteri figlio 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 (come 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. Accedere a **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
   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 figlio e un amministratore blocca alcune impostazioni nel criterio padre, non è possibile modificare queste impostazioni nel criterio figlio.
   - Se si disabilita **Eredita impostazioni dal criterio padre** in un criterio figlio, è possibile modificare tutte le impostazioni nel criterio figlio, anche se alcune impostazioni sono bloccate nel criterio padre.
   - 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 figlio. In questo caso, non è possibile disabilitare questa opzione per nessun criterio figlio. Tutte le impostazioni bloccate nel criterio padre 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 figlio 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 **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 **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).

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. Accedere a **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:
   - Accedere a **DISPOSITIVI** → **DISPOSITIVI GESTITI** → **Gruppi**, quindi selezionare il gruppo di amministrazione che contiene i dispositivi da sincronizzare.
   - Eseguire una selezione dispositivi per visualizzare l'elenco dei dispositivi.
2. Selezionare le caselle di controllo accanto ai dispositivi che si desidera sincronizzare con Administration Server.
3. 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. Accedere a **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 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. Accedere a **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 100000.

Per modificare il numero dei dispositivi visualizzati nell'elenco con i risultati di distribuzione dei criteri:

1. Accedere alla sezione **Opzioni di interfaccia** nella barra degli strumenti.
2. In **Limite di dispositivi visualizzati nei risultati di distribuzione criteri** immettere il numero di dispositivi (fino a 100000).
   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 **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 **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 la 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 per il 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

Espandi tutto | Comprimi tutto

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 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.

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.

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 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.

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 degli accessi in base al ruolo

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**, **Modifica** 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.

> 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**	**Modifica**	• Aggiungere un dispositivo a un gruppo di	Nessuna	Nessuna	Nessuna

		amministrazione: **Modifica** • Eliminare un dispositivo da un gruppo di amministrazione: **Modifica** • Aggiungere un gruppo di amministrazione a un altro gruppo di amministrazione: **Modifica** • Eliminare un gruppo di amministrazione da un altro gruppo di amministrazione: **Modifica**			
Caratteristiche generali: **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi**	**Lettura**	Ottenere l'accesso in lettura a tutti gli oggetti: **Lettura**	Nessuna	Nessuna	Nessuna
Caratteristiche generali: **Funzionalità di base**	• **Lettura** • **Modifica** • **Esecuzione** • **Esegui operazioni per le selezioni di dispositivi**	• Regole di spostamento dei dispositivi (creazione, modifica o eliminazione) per il server virtuale: **Modifica**, **Esegui operazioni per le selezioni dispositivi** • Ottenere un certificato personalizzato per il protocollo Mobile (LWNGT): **Lettura** • Impostare un certificato personalizzato per il protocollo Mobile (LWNGT): **Scrittura** • Ottenere l'elenco di reti definito da NLA: **Lettura** • Aggiungere, modificare o eliminare l'elenco di reti definito da NLA: **Modifica** • Visualizzare gli elenchi di controllo di accesso dei gruppi: **Lettura** • Visualizzare il registro eventi Kaspersky: **Lettura**	• "Scarica aggiornamenti nell'archivio di Administration Server" • "Invia rapporti" • "Distribuisci pacchetto di installazione" • "Installa l'applicazione negli Administration Server secondari in remoto"	• "Rapporto sullo stato della protezione" • "Rapporto sulle minacce" • "Rapporto sui dispositivi più infetti" • "Rapporto sullo stato dei database anti-virus" • "Rapporto sugli errori" • "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	Nessuna

				punti di distribuzione" • "Rapporto sugli Administration Server secondari" • "Rapporto sugli eventi di Controllo Dispositivi" • "Rapporto sulle applicazioni proibite" • "Rapporto su Controllo Web" • "Rapporto sulle autorizzazioni utente effettive" • "Rapporto sui diritti"	
Caratteristiche generali: **Oggetti eliminati**	• **Lettura** • **Modifica**	• Visualizzare gli oggetti eliminati nel Cestino: **Lettura** • Eliminare gli oggetti dal Cestino: **Modifica**	Nessuna	Nessuna	Nessuna
Caratteristiche generali: **Elaborazione degli eventi**	• **Elimina eventi** • **Modifica impostazioni di notifica eventi** • **Modifica impostazioni registro eventi** • **Modifica**	• Modificare le impostazioni di registrazione degli eventi: **Modifica impostazioni registro eventi** • Modificare le impostazioni di notifica degli eventi: **Modifica impostazioni di notifica eventi** • Eliminare gli eventi: **Elimina eventi**	Nessuna	Nessuna	Impostazioni: • Numero massimo di eventi archiviati nel database • Periodo di tempo per l'archiviazione degli eventi dai dispositivi eliminati
Caratteristiche generali: **Operazioni in Administration Server**	• **Lettura** • **Modifica** • **Esecuzione** • **Modifica elenchi di controllo degli accessi agli oggetti** • **Esegui operazioni per le selezioni di dispositivi**	• Specificare le porte dell'Administration Server per la connessione di Network Agent: **Modifica** • Specificare le porte del proxy di attivazione avviato sull'Administration Server: **Modifica** • Specificare le porte del proxy di attivazione per i dispositivi mobili avviato sull'Administration Server: **Modifica** • Specificare le porte del server Web per la distribuzione di	• "Backup dei dati di Administration Server" • "Manutenzione database"	Nessuna	Nessuna

		pacchetti indipendenti: **Modifica** • Specificare le porte del server Web per la distribuzione dei profili MDM: **Modifica** • Specificare le porte SSL dell'Administration Server per la connessione tramite Web Console: **Modifica** • Specificare le porte dell'Administration Server per la connessione mobile: **Modifica** • Specificare il numero massimo di eventi archiviati nel database dell'Administration Server: **Modifica** • Specificare il numero massimo di eventi che possono essere inviati dall'Administration Server: **Modifica** • Specificare il periodo di tempo durante il quale gli eventi possono essere inviati dall'Administration Server: **Modifica**			
Caratteristiche generali: **Distribuzione del software Kaspersky**	• **Gestisci patch di Kaspersky** • **Lettura** • **Modifica** • **Esecuzione** • **Esegui operazioni per le selezioni di dispositivi**	Accettare o rifiutare l'installazione della patch: **Gestisci patch di Kaspersky**	Nessuna	• "Rapporto sull'utilizzo delle chiavi di licenza da parte dell'Administration Server virtuale" • "Rapporto sulle versioni del software Kaspersky" • "Rapporto sulle applicazioni incompatibili" • "Rapporto sulle versioni degli aggiornamenti dei moduli software Kaspersky" • "Rapporto sulla distribuzione della protezione"	Pacchetto di installazione: "Kaspersky"
Caratteristiche generali: **Gestione delle chiavi**	• **Esporta file chiave** • **Modifica**	• Esportare il file chiave: **Esporta file chiave** • Modificare le impostazioni della chiave di licenza di Administration Server: **Modifica**	Nessuna	Nessuna	Nessuna

Caratteristiche generali: **Gestione dei rapporti forzata**	• **Lettura** • **Modifica**	• Creare rapporti indipendentemente dagli elenchi di controllo degli accessi degli oggetti: **Scrittura** • Eseguire rapporti indipendentemente dagli elenchi di controllo degli accessi degli oggetti: **Lettura**	Nessuna	Nessuna	Nessuna
Caratteristiche generali: **Gerarchia di Administration Server**	**Configura gerarchia di Administration Server**	• Registrare, aggiornare o eliminare gli Administration Server secondari: **Configura gerarchia di Administration Server**	Nessuna	Nessuna	Nessuna
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**	Nessuna	Nessuna	Nessuna
Caratteristiche generali: **Administration Server virtuali**	• **Gestisci Administration Server virtuali** • **Lettura** • **Modifica** • **Esecuzione** • **Esegui operazioni per le selezioni di dispositivi**	• Ottenere l'elenco degli Administration Server virtuali: **Lettura** • Ottenere informazioni sull'Administration 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**	Nessuna	Nessuna	Nessuna

- Impostare le autorizzazioni dell'Administration Server virtuale: **Gestisci Administration Server virtuali**

Ruoli utente predefiniti

I ruoli utente assegnati agli utenti di Kaspersky Security Center Linux forniscono set di diritti di accesso alle funzionalità dell'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. 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 **modifica** 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** e **Amministratore/Operatore Mobile Device Management** hanno accesso solo per i diritti dell'area funzionale **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**
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
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**
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**, **Modifica**, **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.

Aggiunta di un account di un utente interno

Per aggiungere un nuovo account utente interno a Kaspersky Security Center Linux:

1. Nel menu principale accedere a **UTENTI E RUOLI** → **UTENTI**.
2. Fare clic su **Aggiungi**.

3. Nella finestra **Nuova entità** visualizzata specificare le impostazioni del nuovo account utente:

   - Mantenere l'opzione predefinita **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.
   - **Nome completo**
   - **Descrizione**
   - **Indirizzo e-mail**
   - **Telefono**

4. Fare clic su **OK** per salvare le modifiche.

Il nuovo account utente verrà visualizzato nell'elenco di utenti e gruppi di utenti.

Creazione di un gruppo di utenti

Per creare un gruppo di utenti:

1. Nel menu principale accedere a **UTENTI E RUOLI** → **UTENTI**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Nuova entità** visualizzata selezionare **Gruppo**.
4. Specificare le seguenti impostazioni per il nuovo gruppo di utenti:
   - **Nome gruppo**
   - **Descrizione**
5. Fare clic su **OK** per salvare le modifiche.

Il nuovo gruppo di utenti verrà visualizzato nell'elenco di utenti e gruppi di utenti.

Modifica di un account di un utente interno

Per modificare un account utente interno in Kaspersky Security Center Linux:

1. Nel menu principale accedere a **UTENTI E RUOLI** → **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**
   - **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 e gruppi di protezione.

Modifica di un gruppo di utenti

> È possibile modificare solo i gruppi interni.

Per modificare un gruppo di utenti:

1. Nel menu principale accedere a **UTENTI E RUOLI** → **UTENTI**.
2. Fare clic sul nome del gruppo di utenti che si desidera modificare.
3. Nella finestra delle impostazioni del gruppo visualizzata modificare le impostazioni del gruppo di utenti:
   - **Nome**
   - **Descrizione**

4. Fare clic su **Salva** per salvare le modifiche.

Il gruppo di utenti aggiornato verrà visualizzato nell'elenco di utenti e gruppi di utenti.

Aggiunta di account utente a un gruppo interno

È possibile aggiungere solo account di utenti interni a un gruppo interno.

Per aggiungere account utente a un gruppo interno:

1. Nel menu principale accedere a **UTENTI E RUOLI** → **UTENTI**.
2. Selezionare le caselle di controllo accanto agli account utente che si desidera aggiungere a un gruppo.
3. Fare clic sul pulsante **Assegna gruppo**.
4. Nella finestra **Assegna gruppo** visualizzata selezionare il gruppo a cui si desidera aggiungere gli account utente.
5. Fare clic sul pulsante **Assegna**.

Gli account utente verranno aggiunti al 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. Nel menu principale accedere a **UTENTI E RUOLI** → **UTENTI**.
2. Fare clic sul nome dell'account utente che si desidera assegnare come proprietario dispositivo.
3. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Dispositivi**.
4. Fare clic su **Aggiungi**.
5. Dall'elenco dei dispositivi selezionare il dispositivo che si desidera assegnare all'utente.
6. Fare clic su **OK**.

Il dispositivo selezionato verrà aggiunto all'elenco dei dispositivi assegnati all'utente.

È possibile eseguire la stessa operazione in **DISPOSITIVI** → **DISPOSITIVI GESTITI**, facendo clic sul nome del dispositivo che si desidera assegnare e quindi facendo clic sul collegamento **Gestisci proprietario dispositivo**.

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 accedere a **UTENTI E RUOLI** → **UTENTI**.
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 accedere a **UTENTI E RUOLI** → **UTENTI**.
2. Selezionare le caselle di controllo accanto agli utenti e 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. Nella pagina **Selezionare un ruolo** della procedura guidata selezionare il ruolo utente che si desidera assegnare.
5. Nella pagina **Definire l'ambito** della procedura guidata selezionare il gruppo di amministrazione da aggiungere all'ambito del ruolo utente.
6. Fare clic sul pulsante **Assegna ruolo** per chiudere la procedura guidata.

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. Nella pagina **Definire l'ambito** della procedura guidata selezionare il gruppo di amministrazione da aggiungere all'ambito del ruolo utente.
6. Nella pagina **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 procedura guidata.
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.

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.

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:

- Administration Server
- Criteri
- Attività
- Gruppi di amministrazione
- Account utente
- Pacchetti di installazione

È possibile eseguire le seguenti azioni sulle revisioni degli oggetti:

- Confrontare una revisione selezionata con quella corrente
- Confrontare le revisioni selezionate
- Confrontare un oggetto con la revisione selezionata di un altro oggetto dello stesso tipo
- Visualizzare una revisione selezionata
- Eseguire il rollback delle modifiche apportate a un oggetto a una revisione selezionata
- Salvare le revisioni come file .txt

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:

- Numero di revisione dell'oggetto
- Data e ora di modifica dell'oggetto
- Nome dell'utente che ha modificato l'oggetto
- Azione eseguita sull'oggetto
- 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 **Descrizione**. Nella finestra **Descrizione revisione oggetto** immettere il testo relativo alla descrizione della revisione.

Informazioni sulle revisioni degli oggetti

È possibile eseguire le seguenti azioni sulle revisioni degli oggetti:

- Confrontare una revisione selezionata con quella corrente
- Confrontare le revisioni selezionate
- Confrontare un oggetto con la revisione selezionata di un altro oggetto dello stesso tipo
- Visualizzare una revisione selezionata
- Eseguire il rollback delle modifiche apportate a un oggetto a una revisione selezionata
- Salvare le revisioni come file .txt

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:

- Numero di revisione dell'oggetto
- Data e ora di modifica dell'oggetto
- Nome dell'utente che ha modificato l'oggetto
- Azione eseguita sull'oggetto
- Descrizione della revisione relativa alla modifica apportata alle impostazioni dell'oggetto

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 e la visualizzazione di informazioni sugli oggetti dopo l'eliminazione.

È possibile eliminare oggetti come:

- Criteri
- Attività
- Pacchetti di installazione
- Administration Server virtuali
- Utenti
- Gruppi di protezione
- Gruppi di amministrazione

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**.

Utilizzo dell'utilità klscflag per aprire la porta 13291

La porta 13291 nell'Administration Server viene utilizzata per ricevere connessioni da Administration Console. Nei computer non Windows, questa porta non è aperta per impostazione predefinita. Se si desidera utilizzare la Administration Console basata su MMC o l'utilità klakaut, è possibile aprire questa porta utilizzando l'utilità klscflag. Questa utilità 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:
   ```
   $ 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:

```
$ 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`.

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 e le applicazioni di protezione

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 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 14 Web Console.
2. Creato e configurato tutti i criteri, i profili dei criteri 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 dei componenti di Kaspersky Security Center e delle 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. 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 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 verifica se i server Kaspersky sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza il DNS pubblico. 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 e le applicazioni di protezione

  Kaspersky Security Center 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:

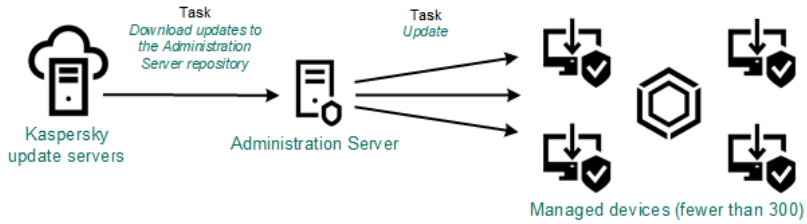
  - Kaspersky Security Center Administration Server, Kaspersky Security Center 14 Web Console
  - Network Agent, Kaspersky Endpoint Security for Linux, plug-in Web di gestione

In base alla configurazione della propria rete è possibile utilizzare i seguenti schemi di download e distribuzione degli aggiornamenti richiesti ai dispositivi gestiti:

- Utilizzando una singola 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 for Linux 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 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).



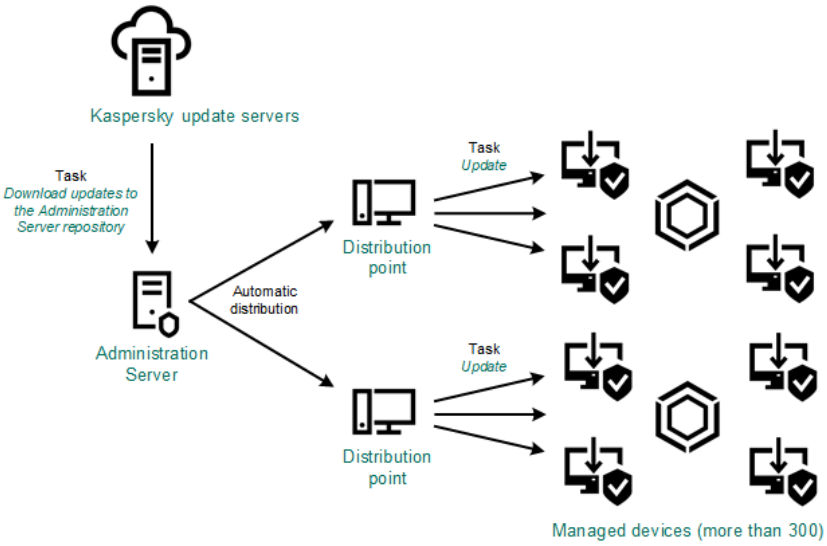
Aggiornamento tramite l'attività Scarica aggiornamenti nell'archivio dell'Administration Server senza punti di distribuzione

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 for Linux vengono scaricati nell'archivio di Administration Server. Questi aggiornamenti vengono installati tramite l'attività di aggiornamento per Kaspersky Endpoint Security for Linux.

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.

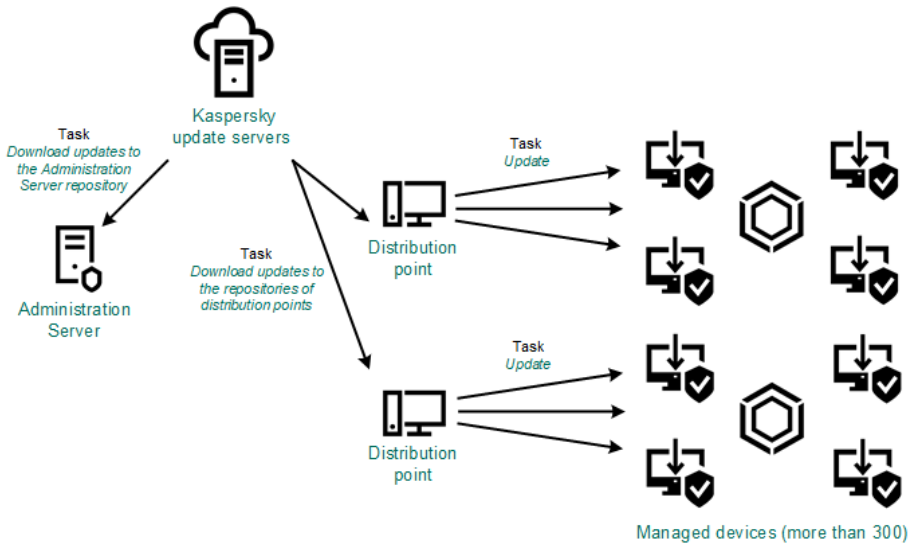
Ogni applicazione Kaspersky richiede gli aggiornamenti necessari da Administration Server. Administration Server aggrega tali richieste e scarica solo gli aggiornamenti che sono richiesti da un'applicazione. Questo garantisce che gli stessi aggiornamenti non vengano scaricati più volte e che gli aggiornamenti 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

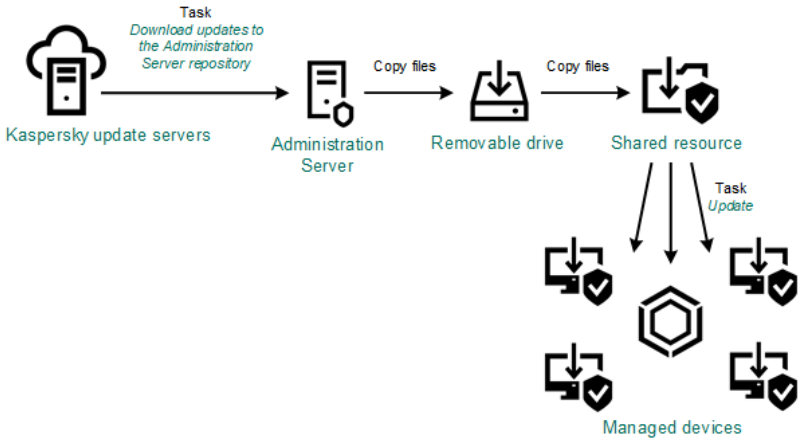
Per impostazione predefinita, Administration Server e i punti di distribuzione comunicano con i server di aggiornamento Kaspersky e scaricano gli aggiornamenti utilizzando il protocollo HTTPS. È possibile configurare Administration Server e/o i punti di distribuzione per fare in modo che utilizzino il 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.

Manualmente attraverso una cartella locale, una cartella condivisa o un server FTP

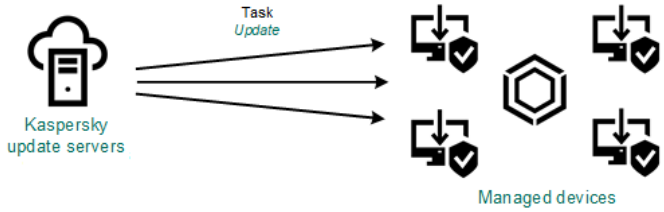
Se i dispositivi client non hanno una connessione ad Administration Server, è possibile utilizzare una cartella locale o una risorsa condivisa come sorgente per l'aggiornamento di database, moduli software e applicazioni Kaspersky. In questo schema è necessario copiare gli aggiornamenti richiesti dall'archivio 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 for Windows (vedere la figura di seguito).



Aggiornamento tramite una cartella locale, una cartella condivisa o un server FTP

Direttamente dai server di aggiornamento Kaspersky a Kaspersky Endpoint Security for Linux nei dispositivi gestiti

Nei dispositivi gestiti è possibile configurare Kaspersky Endpoint Security for Linux 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. 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 una descrizione completa di queste impostazioni, fare riferimento alla documentazione di Kaspersky Endpoint Security for Linux.

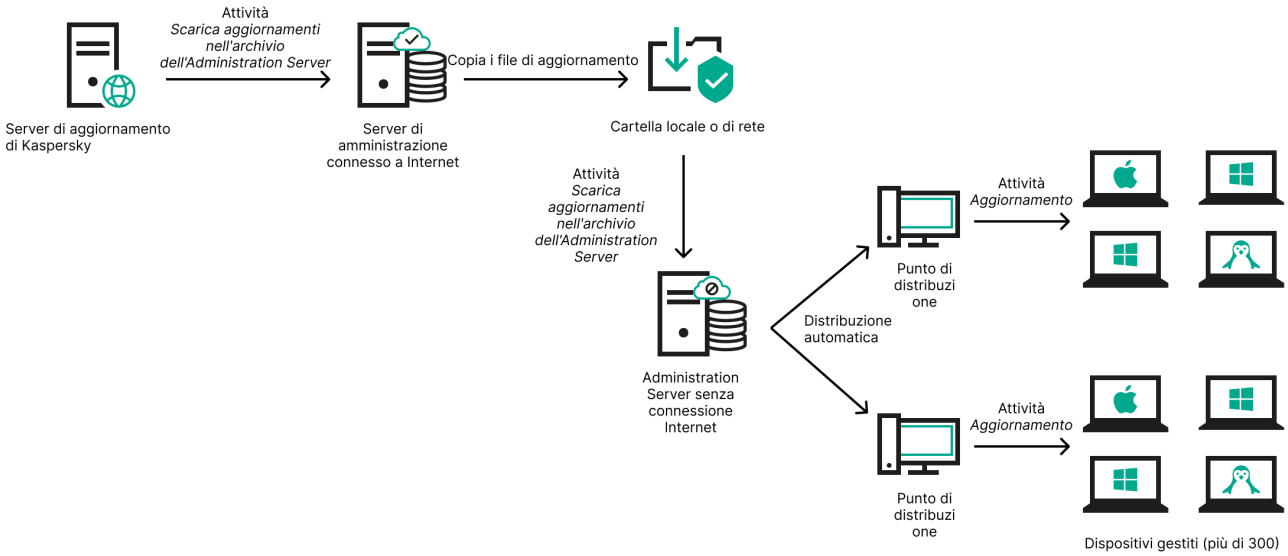
Tramite una cartella locale o di rete se Administration Server non dispone della connessione a Internet

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

Espandi tutto | Comprimi tutto

L'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* consente di scaricare gli aggiornamenti dei database e dei moduli software per le applicazioni di sicurezza 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 **Eseguire 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. Accedere a **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 **Completare la creazione 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 modificarne le impostazioni predefinite. 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 principale.

- **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.

- **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 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 aggiornamenti deve contenere i file di aggiornamento con i metadati compatibili con il nuovo schema. Se la sorgente 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 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.

  - Kaspersky Security Center 13.2 o versione precedente

    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 aggiornamenti per Administration Server 1. Se Administration Server 2 dispone della versione 13.2 o precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente** nell'attività per Administration Server 1.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Eseguire 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**:

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

- **Manualmente** (opzione selezionata per impostazione predefinita)

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è abilitata.

- **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 lunedì 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 18:00:00.

- **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.

- 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, vengono eseguite solo le attività pianificate nei dispositivi client. Per le opzioni **Manualmente**, **Una sola volta** e **Immediatamente**, le attività sono 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 abilitata.

  - **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 dell'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 l'attività se è in esecuzione da 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.

Visualizzazione degli aggiornamenti scaricati

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. È possibile visualizzare gli aggiornamenti scaricati nella sezione **AGGIORNAMENTI PER DATABASE E MODULI SOFTWARE KASPERSKY**.

Per visualizzare l'elenco degli aggiornamenti scaricati:

Nel menu principale accedere a **OPERAZIONI → APPLICAZIONI KASPERSKY → AGGIORNAMENTI PER DATABASE E MODULI SOFTWARE KASPERSKY**.

Verrà visualizzato un elenco degli aggiornamenti disponibili.

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 *Verifica 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 di 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 virus per un'applicazione supportata da Kaspersky Security Center, ad esempio Kaspersky Endpoint Security for Linux. Quando si creano le attività di aggiornamento e scansione virus, specificare il gruppo di amministrazione con i dispositivi di test.

   L'attività *Verifica aggiornamenti* esegue in sequenza le attività di aggiornamento e scansione virus 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 virus.

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 **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 **Eseguire la verifica degli aggiornamenti**.
4. Se l'attività *Verifica aggiornamenti* 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. Nell'Aggiunta guidata 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, quindi selezionare l'attività di scansione virus.

      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 l'opzione **Account predefinito** abilitata. 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

Espandi tutto | Comprimi tutto

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 **DISPOSITIVI** → **ATTIVITÀ**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata l'Aggiunta guidata 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. Durante il passaggio **Completare la creazione 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. Una cartella di rete può essere un server FTP o HTTP oppure una condivisione SMB. Se una cartella di rete richiede l'autenticazione, è supportato solo il protocollo SMB. Quando si seleziona una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server.

  > Una cartella di rete o un server FTP o HTTP utilizzato da una sorgente aggiornamenti deve contenere una struttura di cartelle (con gli aggiornamenti) che corrisponde alla struttura creata durante l'utilizzo dei server di aggiornamento Kaspersky.

Se si abilita l'opzione **Non usare server proxy** per le sorgenti degli aggiornamenti Server degli aggiornamenti Kaspersky o Cartella locale o di rete, un punto di distribuzione non utilizza un server proxy per il download degli aggiornamenti, anche se è stata abilitata l'opzione **Usa server proxy** delle impostazioni del criterio di Network Agent per il punto di distribuzione.

- **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 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 aggiornamenti deve contenere i file di aggiornamento con i metadati compatibili con il nuovo schema. Se la sorgente 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 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.

  - Kaspersky Security Center 13.2 o versione precedente

    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 13.2 o precedente, 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**:

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Manualmente** (opzione selezionata per impostazione predefinita)

    L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

    Per impostazione predefinita, questa opzione è abilitata.

  - **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 lunedì 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 18:00:00.

- **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 anti-virus 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.

- **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, vengono eseguite solo le attività pianificate nei dispositivi client. Per le opzioni **Manualmente**, **Una sola volta** e **Immediatamente**, le attività sono 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 abilitata.

- **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 dell'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 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

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 possibile utilizzare solo una cartella sull'Administration Server; come cartella di rete, è possibile utilizzare solo un server FTP o HTTP.

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.

Nel caso in cui una cartella condivisa che contiene aggiornamenti sia protetta da password, abilitare l'opzione **Specifica l'account per accedere alla cartella condivisa della sorgente degli aggiornamenti (se disponibile)** e inserire le credenziali dell'account necessarie per l'accesso.

Per aggiungere le sorgenti degli aggiornamenti:

1. Accedere a **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.

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: scenario

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** delle proprietà dell'Administration Server.

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. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** () accanto al nome dell'Administration Server desiderato.

   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 dall'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 l'Aggiunta guidata 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 di Administration Server contenga gli aggiornamenti richiesti per l'applicazione di sicurezza installata in un dispositivo offline, in almeno uno dei dispositivi online gestiti deve essere installata la stessa applicazione di sicurezza. 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 sicurezza per la ricezione degli aggiornamenti dall'archivio di 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: \\<nome server>\KLSHARE\Updates.

   In alternativa, è possibile configurare Kaspersky Security Center 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 for Linux) per la ricezione degli aggiornamenti da una cartella locale o una risorsa condivisa, come un server FTP o una cartella condivisa.
4. Copiare i file degli aggiornamenti dall'unità rimovibile nella cartella locale o nella risorsa condivisa che si desidera utilizzare come sorgente aggiornamenti.
5. Nel dispositivo offline che richiede l'installazione degli aggiornamenti avviare l'attività di aggiornamento di Kaspersky Endpoint Security for Linux.

Al termine dell'attività di aggiornamento, i database e i moduli software Kaspersky sono aggiornati nel dispositivo.

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:

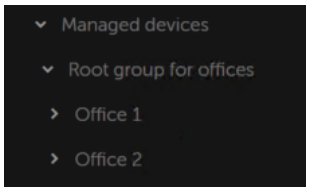
- Creazione della struttura dei gruppi di amministrazione tenendo conto della topologia di rete. La struttura dei gruppi di amministrazione potrebbe non riflettere la topologia di rete alla perfezione. Una corrispondenza tra i diversi componenti della rete e alcuni gruppi di amministrazione può essere 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/5000 + 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/5000 + 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. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** () accanto al nome dell'Administration Server desiderato.

   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

Espandi tutto | Comprimi tutto

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. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** () accanto al nome dell'Administration Server desiderato.

   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. Selezionare il 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.

     - **Numero di 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.

     - **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.

- 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 dall'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 l'Aggiunta guidata 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.
- Configurare il polling degli intervalli IP da parte del punto di distribuzione.
  - **Intervalli IP**

    Adesso è possibile abilitare Device discovery per gli intervalli IPv4 e le reti IPv6.

    Se si abilita l'opzione **Abilita polling intervalli**, 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 **Abilita il polling con la tecnologia Zeroconf**, 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.
- 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. Accedere a **DISPOSITIVI** → **Gruppi**.
2. Nella struttura dei gruppi di amministrazione selezionare il gruppo di amministrazione per cui si desidera visualizzare i punti di distribuzione assegnati.

3. Fare clic sulla scheda **PUNTI DI DISTRIBUZIONE**.

4. Aggiungere nuovi punti di distribuzione per il gruppo di amministrazione utilizzando il pulsante **Assegna** o rimuovere i punti di distribuzione assegnati utilizzando il 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 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 possibile utilizzare i punti di distribuzione come server push per garantire la connettività continua tra un dispositivo gestito e Administration Server. La connettività continua 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. Fare clic sull'icona **Impostazioni** (⚙) accanto al nome dell'Administration Server desiderato.
   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.

Gestione delle applicazioni di terze parti nei dispositivi client

Questa sezione descrive le funzionalità di Kaspersky Security Center Linux correlate alla gestione delle applicazioni di terze parti eseguite nei dispositivi client.

Scenario: Gestione applicazioni

È possibile gestire l'avvio delle applicazioni nei dispositivi degli utenti. È possibile consentire o bloccare l'esecuzione delle applicazioni nei dispositivi gestiti. Questa funzionalità è resa possibile dal componente Controllo Applicazioni.

Il componente Controllo Applicazioni è disponibile per Kaspersky Endpoint Security 11.2 for Linux e versioni successive.

Prerequisiti

- Kaspersky Security Center Linux viene distribuito nell'organizzazione.
- Il criterio di Kaspersky Endpoint Security for Linux è stato creato ed è attivo.

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. È possibile ignorare questo passaggio se si sa esattamente quali file eseguibili sono presenti nei dispositivi gestiti.

Istruzioni dettagliate: Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client

2. **Creazione delle categorie di applicazioni per le applicazioni utilizzate nell'organizzazione**

   Analizzare gli elenchi dei file eseguibili archiviati nei dispositivi gestiti. In base all'analisi, creare le categorie di applicazioni. È consigliabile creare una categoria "Applicazioni di lavoro" che includa il set standard di applicazioni utilizzate nell'organizzazione. Se differenti gruppi di utenti utilizzano diversi set di applicazioni nel proprio lavoro, è possibile creare una categoria di applicazioni distinta per ciascun gruppo di utenti.

   Istruzioni dettagliate: Creazione di una categoria di applicazioni con contenuto aggiunto manualmente

3. **Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Linux**

   Configurare il componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Linux utilizzando le categorie di applicazioni create nel passaggio precedente.

4. **Verifica della configurazione di Controllo Applicazioni**

   Assicurarsi di avere eseguito le seguenti operazioni:

   - Creazione delle categorie di applicazioni.
   - Configurazione di Controllo Applicazioni tramite le categorie di applicazioni.

Risultati

Al termine dello scenario, viene controllato l'avvio delle applicazioni nei dispositivi gestiti. Gli utenti possono avviare solo le applicazioni consentite nell'organizzazione, mentre non possono avviare quelle non consentite.

Per informazioni dettagliate su Controllo Applicazioni, consultare la Guida in linea di Kaspersky Endpoint Security for Linux.

Informazioni su Controllo Applicazioni

Il componente Controllo Applicazioni monitora i tentativi degli utenti di avviare le applicazioni e regola l'avvio delle applicazioni tramite le regole di Controllo Applicazioni.

> Il componente Controllo Applicazioni è disponibile per Kaspersky Endpoint Security 11.2 for Linux e versioni successive.

L'avvio delle applicazioni 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 tutte le applicazioni tranne quelle specificate nelle regole di blocco. Questa modalità è selezionata per impostazione predefinita.
- *Lista consentiti*. La modalità viene utilizzata se si desidera bloccare l'avvio di tutte le applicazioni tranne quelle specificate nelle regole di permesso.

Le regole di Controllo Applicazioni sono implementate attraverso categorie di applicazioni. Le categorie di applicazioni vengono create definendo criteri specifici. In Kaspersky Security Center Linux, è possibile creare solo categorie con contenuto aggiunto manualmente. Vengono definite le condizioni (ad esempio, metadati del file, codice hash del file, certificato del file, categoria KL o percorso del file) per includere i file eseguibili nella categoria.

Per informazioni dettagliate su Controllo Applicazioni, consultare la Guida in linea di Kaspersky Endpoint Security for Linux.

Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client

È possibile ottenere un elenco di file eseguibili archiviati nei dispositivi gestiti. Per eseguire un inventario dei file eseguibili, è necessario creare un'attività di inventario.

> La funzionalità di inventario dei file eseguibili è disponibile per Kaspersky Endpoint Security 11.2 for Linux e versioni successive.

Per creare un'attività di inventario per i file eseguibili nei dispositivi client:

1. Accedere a **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.

4. Nell'elenco a discesa **Tipo di attività** selezionare **Inventario**.

5. Nella pagina **Completare la creazione dell'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, fare riferimento alla Guida in linea di Kaspersky Endpoint Security for Linux.

Dopo l'esecuzione dell'attività **Inventario**, viene formato l'elenco dei file eseguibili archiviati nei dispositivi gestiti ed è possibile visualizzarlo.

Durante l'inventario, vengono rilevati i file eseguibili nei seguenti formati: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Per visualizzare l'elenco dei file eseguibili archiviati nei dispositivi client:

Nell'elenco a discesa **OPERAZIONI → APPLICAZIONI DI TERZE PARTI** selezionare **FILE ESEGUIBILI**.

La pagina visualizzerà l'elenco dei file eseguibili archiviati nei dispositivi client.

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. Nell'elenco a discesa **OPERAZIONI → APPLICAZIONI DI TERZE PARTI** selezionare **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. Seguire le istruzioni della procedura guidata.

3. Nella pagina **Selezionare il metodo di creazione della categoria** della procedura guidata selezionare l'opzione **Categoria con contenuto aggiunto manualmente. I dati dei file eseguibili vengono aggiunti alla categoria in modo manuale**.

4. Nella pagina **Condizioni** della procedura guidata fare clic sul pulsante **Aggiungi** per aggiungere un criterio di condizione per includere i file nella creazione della categoria.

5. Nella pagina **Criteri condizione** selezionare un tipo di regola per la creazione della categoria dall'elenco:

   - Seleziona certificato dall'archivio

     Se questa opzione è selezionata, è possibile specificare i certificati dell'archivio. I file eseguibili firmati in base ai certificati specificati verranno aggiunti alla categoria utente.

   - 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. È possibile selezionare un'applicazione dal registro e specificare i seguenti metadati dei file:

  - 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.

- **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 vengono archiviate nel database di Administration Server. L'archiviazione dei valori hash non aumenta in modo significativo le dimensioni del database.

  SHA-256 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 SHA-256.

  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. I metadati verranno inviati ad Administration Server. I file eseguibili che contengono gli stessi metadati verranno aggiunti alla categoria di applicazioni.

  Certificato

  Se questa opzione è selezionata, è possibile specificare i certificati dell'archivio. I file eseguibili firmati in base ai certificati specificati verranno aggiunti alla categoria utente.

- **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 SHA-256) 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. Nella pagina **Esclusioni** della procedura guidata fare clic sul pulsante **Aggiungi** per aggiungere un criterio di condizione esclusivo per escludere i file dalla categoria creata.

7. Nella pagina **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 in linea di Kaspersky Endpoint Security for Linux.

Visualizzazione dell'elenco delle categorie di applicazioni

È possibile visualizzare l'elenco delle categorie di applicazioni configurate e le impostazioni di ciascuna categoria di applicazioni.

Per visualizzare l'elenco delle categorie di applicazioni:

Nella scheda **OPERAZIONI**, nell'elenco a discesa **APPLICAZIONI DI TERZE PARTI**, selezionare **CATEGORIE DI APPLICAZIONI**.

Verrà visualizzata la pagina con un elenco di categorie di applicazioni.

Per visualizzare le proprietà di una categoria di applicazioni:

Fare clic sul nome della categoria di applicazioni.

Verrà visualizzata la finestra delle proprietà della categoria di applicazioni. Le proprietà sono raggruppate in diverse schede.

Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni

Espandi tutto | Comprimi tutto

Dopo aver configurato Controllo Applicazioni nei criteri di Kaspersky Endpoint Security for Linux, 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 per il blocco dell'avvio di un'applicazione** (evento *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. 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 SHA-256 univoca. Quando si seleziona una funzione hash SHA-256, 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 SHA-256 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 SHA-256 univoca. Quando si seleziona una funzione hash SHA-256, 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 SHA-256 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 in linea di Kaspersky Endpoint Security for Linux.

Monitoraggio e generazione di rapporti

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 di 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 di 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 14 Web Console fornisce i seguenti tipi di monitoraggio e generazione di 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 14 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 14 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 14 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 **Aggiungere o ripristinare 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 **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 **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 **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 **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).

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 (ad esempio un Top Manager). Quando per un utente è abilitata questa modalità, viene visualizzato solo un dashboard con un set predefinito di widget. L'utente potrà 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 E RUOLI → UTENTI**. 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 accedere a **UTENTI E RUOLI → 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 tal fine, nella scheda **Dashboard** è possibile eseguire con i widget le stesse azioni possibili nella 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, 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 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 14 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. Nella prima pagina della procedura guidata immettere il nome del rapporto e selezionare il tipo di rapporto.
4. Nella pagina **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. Nella pagina **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.

       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. Fare clic sul pulsante **Chiudi** (✕) per 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 esportare un rapporto in un file XML o HTML.

Per esportare un rapporto in un file:

1. Accedere a **MONITORAGGIO E GENERAZIONE DEI RAPPORTI → RAPPORTI**.
2. Selezionare la casella di controllo accanto al rapporto che si desidera esportare in un file.
3. Fare clic sul pulsante **Esporta rapporto**.
4. Nella finestra visualizzata modificare il nome del file del rapporto nel campo **Nome**. Per impostazione predefinita, il nome del file coincide con il nome del modello di rapporto selezionato.
5. Selezionare il tipo di file del rapporto: XML, HTML 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.

6. Fare clic sul pulsante **Esporta rapporto**.

   Il rapporto nel formato selezionato verrà scaricato nel dispositivo (nella cartella predefinita del dispositivo) o verrà visualizzata una finestra **Salva con nome** standard nel browser per consentire di salvare il file nella posizione desiderata.

Il rapporto verrà salvato nel file.

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.

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. 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, se i rapporti salvati precedentemente in questa cartella devono essere sovrascritti e se deve essere utilizzato un account specifico per accedere alla cartella (per una cartella condivisa).
7. Se si desidera modificare altre impostazioni dell'attività dopo averla creata, nella pagina **Completare la creazione dell'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.

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 14 Web Console.

Le selezioni eventi sono disponibili in Kaspersky Security Center 14 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**
  - **Messaggi 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.

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 aperta 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

Per esportare gli eventi in un file:

1. Avviare una selezione eventi.
2. Selezionare la casella di controllo accanto all'evento desiderato.
3. Fare clic sul pulsante **Esporta in un file**.

L'evento selezionato verrà esportato in un file.

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 di tempo 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 di rapporti per un periodo di tempo superiore.

Per impostare il periodo di archiviazione per un evento nel database di Administration Server:

1. Selezionare **DISPOSITIVI → CRITERI E PROFILI**.
2. Eseguire una delle seguenti operazioni:
   - Per configurare il periodo di archiviazione degli eventi di Network Agent o di un'applicazione Kaspersky gestita, fare clic sul nome del criterio corrispondente.

     Verrà visualizzata la pagina delle proprietà del criterio.
   - Per configurare gli eventi di Administration Server, nella parte superiore dello schermo fare clic sull'icona **Impostazioni** () accanto al nome dell'Administration Server desiderato.

     Se si dispone di un criterio per Administration Server, è possibile fare clic sul nome di questo criterio.

     Verrà visualizzata la pagina delle proprietà di Administration Server (o la pagina delle proprietà del criterio di Administration Server).
3. Selezionare la scheda **Configurazione eventi**.

   Verrà visualizzato un elenco dei tipi di eventi correlati alla sezione **Critico**.
4. Selezionare la sezione **Errore funzionale**, **Avviso** o **Informazioni**.
5. 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'opzione **Archivia nel database di Administration Server per (giorni)** è abilitata.
6. Nella casella di modifica sotto questo interruttore inserire il numero di giorni per l'archiviazione dell'evento.
7. 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 Linux Administration Server, non è possibile ridefinire il valore del periodo di archiviazione per un evento.
8. Fare clic su **OK**.

   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.

Tipi di evento

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 Linux. I tipi di eventi che si verificano nelle applicazioni Kaspersky non sono elencati in questa sezione.

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 terze parti 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 Linux Administration Server con il livello di importanza **Critico**.

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 stata superata una limitazione di licenza. 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 superata una limitazione di licenza.	180 giorni
Il dispositivo è diventato non gestito	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 di tempo specifico. 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.	180 giorni
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	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	180 giorni

stato aggiunto alla lista vietati			lista vietati. Contattare il Servizio di assistenza tecnica per ulteriori dettagli.	
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 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 aggiuntiva 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. È possibile configurare gli aggiornamenti automatici dei certificati selezionando la casella di controllo **Riemetti automaticamente il certificato se possibile** nelle impostazioni di emissione del certificato.	180 giorni

Eventi di errore funzionale di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Linux Administration Server con il livello di importanza **Errore funzionale**.

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
Limite di installazioni superato per uno dei gruppi di applicazioni concesse in licenza	4126	KLSRV_INVLICPROD_EXCEDED	Administration Server genera periodicamente eventi di questo tipo (ogni ora). Eventi di questo tipo si verificano se in Kaspersky Security Center Linux si gestiscono chiavi di licenza di applicazioni di terze parti e se il numero di installazioni ha superato il limite impostato dalla chiave di licenza dell'applicazione di terze parti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare l'applicazione di terze parti dai dispositivi in cui non è in uso l'applicazione. • Utilizzare una licenza di terze parti per altri dispositivi.	180 giorni

			È possibile gestire le chiavi di licenza di applicazioni di terze parti utilizzando le funzionalità dei gruppi di applicazioni concesse in licenza. Un gruppo di applicazioni concesse in licenza include le applicazioni di terze parti che soddisfano i criteri impostati dall'utente.	
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 SQL Server. • Visualizzare i log DBMS per scoprire il motivo della mancata disponibilità di Administration Server. A causa della manutenzione preventiva, un server remoto in cui è installato SQL Server potrebbe ad esempio non essere disponibile.	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: • Si utilizza il DBMS SQL Server Express Edition:	180 giorni

- 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 abbia superato 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 for Linux 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.

Eventi di avviso di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Linux Administration Server con il livello di importanza **Avviso**.

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 superato il limite di licenze	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una volta al giorno Kaspersky Security Center Linux verifica se è stata superata una limitazione di licenza. 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 superata una limitazione di licenza.	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.	90 giorni

			È possibile rispondere all'evento nei seguenti modi: • Rimuovere manualmente il dispositivo dall'elenco dei dispositivi gestiti. 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 14 Web Console. • Specificare l'intervallo di tempo dopo il quale il dispositivo viene automaticamente rimosso dal gruppo utilizzando Kaspersky Security Center 14 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 limite di installazioni sta per essere superato per uno dei gruppi di applicazioni concesse in licenza	4127	KLSRV_INVLICPROD_FILLED	Eventi di questo tipo si verificano quando il numero di installazioni per applicazioni di terze parti incluse in un gruppo di applicazioni concesse in licenza raggiunge il 90% del valore massimo consentito specificato nelle proprietà della chiave di licenza. È possibile rispondere all'evento nei seguenti modi: • Se l'applicazione di terze parti non è in uso in alcuni dei dispositivi gestiti, eliminare l'applicazione da questi dispositivi. • Se si prevede che il numero di installazioni per l'applicazione di terze parti supererà il valore massimo consentito nell'immediato futuro, valutare la possibilità di ottenere in anticipo una licenza di terze parti per un numero superiore di dispositivi. È possibile gestire le chiavi di licenza di applicazioni di terze parti utilizzando le funzionalità dei gruppi di applicazioni concesse in licenza.	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	90 giorni

			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.	
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).	90 giorni

			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.	
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 Administration Server si esaurisce quasi totalmente lo spazio disponibile. Liberare spazio su disco nel dispositivo.	90 giorni
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 for Linux 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	90 giorni

			• Ridurre l'elenco degli eventi da archiviare nel database di Administration Server Rivedere le informazioni sulla selezione DBMS.	
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 eventi Kaspersky 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 eventi Kaspersky 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: • Cambiare il numero massimo di eventi archiviati nel database di Administration Server • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server	Non archiviato
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 Linux Administration Server con il livello di importanza **Informazioni**.

Eventi informativi di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito

Utilizzo della chiave di licenza superiore al 90%	4097	KLSRV_EV_LICENSE_CHECK_90	30 giorni
Nuovo dispositivo rilevato	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 giorni
Il dispositivo è stato aggiunto automaticamente al gruppo	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 giorni
Il dispositivo è stato rimosso dal gruppo poiché inattivo nella rete per molto tempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 giorni
Sta per essere superato il limite di installazioni (è stato utilizzato più del 95%) per uno dei gruppi di applicazioni concesse in licenza	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 giorni
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
Controllo: l'oggetto è stato modificato	4148	KLAUD_EV_OBJECTMODIFY	30 giorni
Controllo: lo stato dell'oggetto è stato modificato	4150	KLAUD_EV_TASK_STATE_CHANGED	30 giorni
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
Controllo: le autorizzazioni dell'utente sono state modificate	4153	KLAUD_EV_OBJECTACLMODIFIED	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 Kaspersky Security Center Linux Network Agent con il livello di criticità **Avviso**.

Eventi di avviso di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Si è verificato un incidente	549	GNRL_EV_APP_INCIDENT_OCCURED	30 giorni

Eventi informativi di Network Agent

La tabella seguente elenca gli eventi di Kaspersky Security Center Linux Network Agent con il livello di criticità **Informazioni**.

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

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 vedere 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. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** ( ) accanto al nome dell'Administration Server desiderato.
   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. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** ( ) accanto al nome dell'Administration Server desiderato.
   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.

Se il numero di eventi nel database raggiunge il valore massimo specificato dall'amministratore, l'applicazione elimina gli eventi meno recenti e li sovrascrive con quelli nuovi. Quando l'Administration Server elimina gli eventi meno recenti, non può salvare i nuovi eventi nel database. Durante questo periodo di tempo, le informazioni sugli eventi rifiutati vengono scritte nel registro eventi Kaspersky. I nuovi eventi vengono accodati e quindi salvati nel database al termine dell'operazione di eliminazione.

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 14 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 **Aggiungere o ripristinare 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	Più di 0.

	esempio l'attività Scansione virus, e il numero di virus trovati supera il valore specificato.	
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 virus non eseguita da molto tempo	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma l'attività Scansione virus non viene eseguita 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.
Incidenti non elaborati rilevati	Sono stati rilevati nel dispositivo alcuni incidenti non elaborati. Gli incidenti 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 l'individuazione dispositivi, 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.	Più di 0 minuti.
Applicazione di	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma non	

protezione non in esecuzione	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 **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 padre.

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 **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 padre.

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*.

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. Nella parte superiore dello schermo fare clic sull'icona **Impostazioni** ( ) accanto al nome dell'Administration Server desiderato.

   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 prova** 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 la notifica** 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 prova** 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 la notifica** 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 la notifica** 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 dell'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.

Segnaposto per la descrizione di un evento

Segnaposto	Descrizione del segnaposto
%SEVERITY%	Livello di importanza evento
%COMPUTER%	Nome del dispositivo in cui si è verificato l'evento
%DOMAIN%	Dominio
%EVENT%	Evento
%DESCR%	Descrizione evento
%RISE_TIME%	Ora creazione
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nome attività
%KL_PRODUCT%	Kaspersky Security Center Linux Network Agent
%KL_VERSION%	Numero di versione di Network Agent
%HOST_IP%	Indirizzo IP
%HOST_CONN_IP%	Indirizzo IP connessione

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 di 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 → Annunci Kaspersky**) consente di rimanere informati fornendo informazioni relative alla versione in uso di Kaspersky Security Center e alle applicazioni gestite installate nei dispositivi gestiti. Kaspersky Security Center aggiorna periodicamente le informazioni nella sezione rimuovendo gli annunci obsoleti e aggiungendo nuove informazioni.

Kaspersky Security Center 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 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 Kaspersky 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 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.

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 14 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 → Annunci Kaspersky**) consente di rimanere informati fornendo informazioni relative alla versione in uso di Kaspersky Security Center e alle applicazioni gestite installate nei dispositivi gestiti. Se non si desidera ricevere gli annunci di Kaspersky, è possibile disabilitare questa funzionalità.

Per disabilitare gli annunci di Kaspersky:

1. Nella finestra principale dell'applicazione fare clic sull'icona **Impostazioni** ( ) accanto al nome dell'Administration Server desiderato.

   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.

Esportazione di eventi nei sistemi SIEM

Questa sezione descrive come configurare l'esportazione degli eventi nei sistemi SIEM.

Scenario: 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

Espandi tutto | Comprimi tutto

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 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. È possibile esportare queste informazioni in sistemi SIEM esterni. L'esportazione delle informazioni sugli eventi nei sistemi SIEM esterni consente agli amministratori dei sistemi SIEM di rispondere tempestivamente agli eventi del sistema di protezione che si verificano nei dispositivi o nei gruppi di dispositivi gestiti.

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.

Informazioni sull'esportazione degli eventi

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 terze parti, 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**

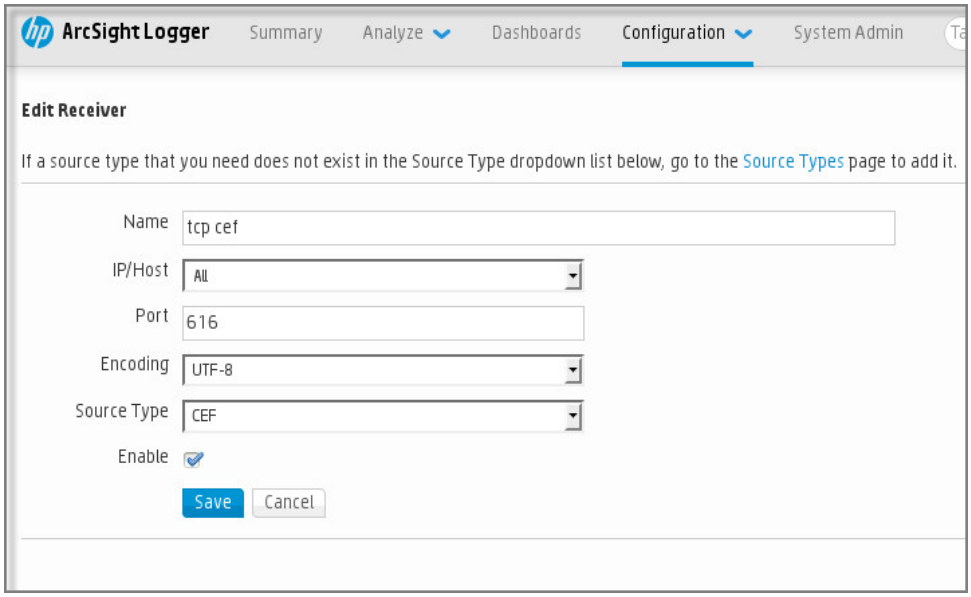
  Specificare il numero di porta per la connessione a Kaspersky Security Center Linux. Deve trattarsi della stessa porta specificata in Kaspersky Security Center Linux durante la configurazione con un sistema SIEM.

- **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, la gravità, la descrizione, i parametri e così via. 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.

Ogni sistema SIEM contiene un set di parser dei messaggi standard. Kaspersky offre inoltre parser dei messaggi per alcuni sistemi SIEM, ad esempio QRadar e ArcSight. È possibile scaricare questi parser dei messaggi dai siti Web dei sistemi SIEM corrispondenti. Durante la configurazione del ricevitore, è possibile scegliere di utilizzare uno dei parser dei messaggi standard o un parser dei messaggi di Kaspersky.

Contrassegno degli eventi per l'esportazione nei sistemi SIEM in formato Syslog

Questa sezione descrive come contrassegnare gli eventi per un'ulteriore esportazione nei sistemi SIEM in formato Syslog.

Informazioni sul contrassegno degli eventi per l'esportazione nel sistema 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 **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. Passare 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 **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. Passare alla sezione **Applicazioni**.
4. Fare clic sul collegamento con il nome dell'applicazione desiderata nell'elenco delle applicazioni.
5. Passare 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 al sistema SIEM gli eventi contrassegnati 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:
   - Fare clic sull'icona **Impostazioni** () accanto al nome dell'Administration Server desiderato.
   - Nel menu principale accedere a **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 al sistema SIEM gli eventi contrassegnati 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

Espandi tutto | Comprimi tutto

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 14 Web Console:

1. Nell'elenco a discesa **Impostazioni della console** selezionare **Integrazione**.

   Verrà aperta la finestra **Impostazioni della console**.

2. Selezionare la scheda **Integrazione**.
3. Nella scheda **Integrazione** selezionare la sezione **SIEM**.
4. Fare clic sul collegamento **Impostazioni**.

   Si aprirà la sezione **Esporta impostazioni**.

5. 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/IP, 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 un file con l'elenco dei certificati da un'autorità di certificazione (CA) attendibile e caricare il file in Kaspersky Security Center Linux. Kaspersky Security Center Linux verifica se anche il certificato del server di sistema SIEM è firmato 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 SHA-1 dei certificati di sistema SIEM in Kaspersky Security Center Cloud Console. Per aggiungere un'identificazione personale SHA-1, inserirla 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. Pertanto, verrà utilizzato un certificato autofirmato emesso da Kaspersky Security Center. 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.

    - **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 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. 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.

6. 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**.

7. Spostare l'opzione sulla posizione **Esporta automaticamente gli eventi nel database del sistema SIEM ABILITATO**.

8. 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 la creazione 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.

Creazione di una query SQL tramite l'utilità klsql2

Questa sezione descrive come scaricare e utilizzare l'utilità klsql2 e come creare una query SQL utilizzando questa utilità. Quando si crea una query SQL tramite l'utilità klsql2, non è necessario specificare il nome del database e i parametri di accesso, perché la query fa direttamente riferimento alle visualizzazioni pubbliche di Kaspersky Security Center Linux.

Per scaricare e utilizzare l'utilità klsql2:

1. Scaricare l'utilità klsql2 dal sito Web di Kaspersky.
2. Copiare ed estrarre il file klsql2.zip scaricato in una cartella nel dispositivo in cui è installato Kaspersky Security Center Linux Administration Server.
   Il pacchetto klsql2.zip contiene i seguenti file:
   - klsql2.exe
   - src.sql
   - start.cmd
3. Aprire il file src.sql in qualsiasi editor di testo.
4. Nel file src.sql digitare la query SQL desiderata e salvare il file.
5. Nel dispositivo in cui è installato Kaspersky Security Center Linux Administration Server digitare nella riga di comando il seguente comando per eseguire la query SQL dal file src.sql e salvare i risultati nel file result.xml:
   ```
   klsql2 -i src.sql -o result.xml
   ```
6. Aprire il file result.xml creato per visualizzare i risultati della query.

È possibile modificare il file src.sql e creare qualsiasi query 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, creata tramite l'utilità klsql2.

Il seguente esempio illustra 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:

```
SELECT
e.nId, /* identificatore dell'evento */
e.tmRiseTime, /* ora in cui si è verificato l'evento */
e.strEventType, /* nome interno del tipo di evento */
```

```
    e.wstrEventTypeDisplayName, /* nome visualizzato dell'evento */
    e.wstrDescription, /* descrizione visualizzata dell'evento */
    e.wstrGroupName, /* nome del gruppo a cui appartiene il dispositivo */
    h.wstrDisplayName, /* nome visualizzato del dispositivo in cui si è verificato l'evento */
    CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
    CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
    CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +
    CAST(((h.nIp) & 255) AS varchar(4)) as strIp /* Indirizzo IP del dispositivo in cui si è verificato l'evento */
    FROM v_akpub_ev_event e
    INNER JOIN v_akpub_host h ON h.nId=e.nHostId
    WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
    ORDER BY e.tmRiseTime DESC
```

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 SQL Server, 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. Fare clic sull'icona **Impostazioni** () accanto al nome dell'Administration Server desiderato.

   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.

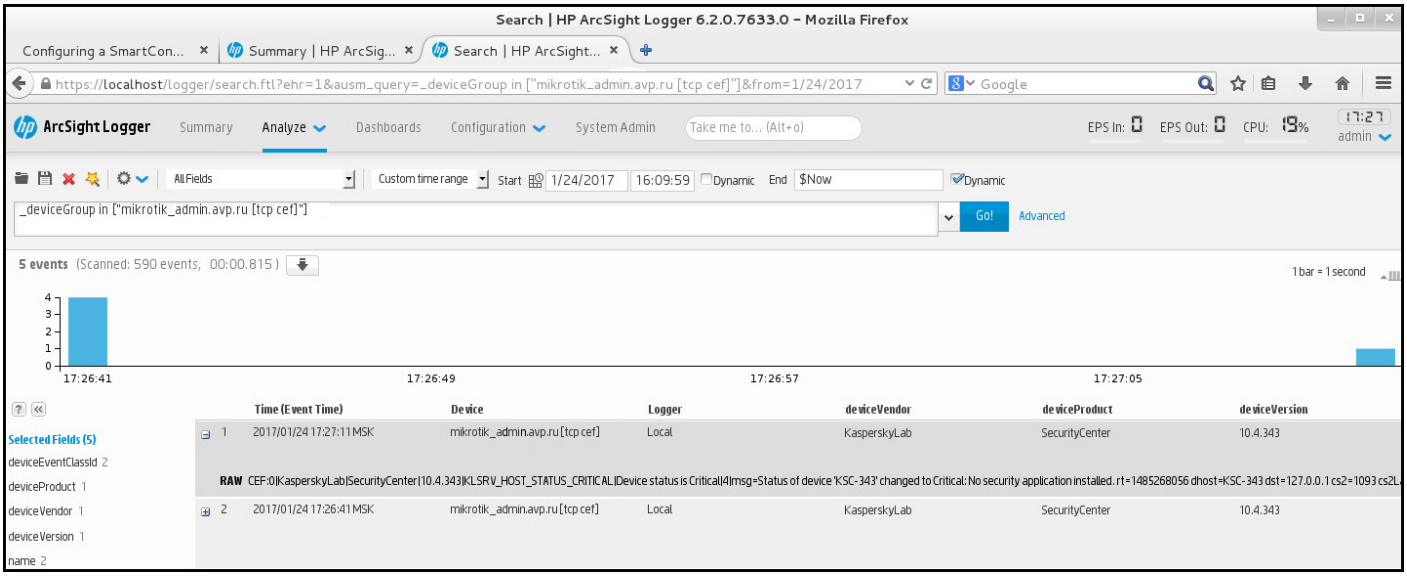
Visualizzazione dei risultati dell'esportazione

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

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 offre un'ampia gamma di *selezioni predefinite* (ad esempio **Dispositivi con stato Critico**, **Protezione disattivata** o **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.

Per visualizzare la selezione dispositivi:

1. Nel menu principale accedere alla sezione **DISPOSITIVI → SELEZIONI DISPOSITIVI** o **INDIVIDUAZIONE E DISTRIBUZIONE → SELEZIONI DISPOSITIVI**.
2. Nell'elenco delle selezioni fare clic sul nome della selezione pertinente.

Verrà visualizzato il risultato della selezione dispositivi.

Creazione di una selezione dispositivi

Per creare una selezione dispositivi:

1. Nel menu principale accedere a **DISPOSITIVI → SELEZIONI DISPOSITIVI**.

   Verrà visualizzata una pagina con un elenco di selezioni dispositivi.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà aperta la finestra **Impostazioni della selezione dispositivi**.
3. Immettere il nome della nuova selezione.
4. Specificare il tipo di dispositivi che si desidera includere nella selezione dispositivi.
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

Espandi tutto | Comprimi tutto

Per configurare una selezione dispositivi:

1. Accedere a **DISPOSITIVI → SELEZIONI DISPOSITIVI**.

   Verrà visualizzata una pagina con un elenco di selezioni dispositivi.
2. Fare clic sulla selezione dispositivi definita dall'utente appropriata.

   Verrà aperta la finestra **Impostazioni della selezione dispositivi**.
3. Nella scheda **Generale** specificare le condizioni da soddisfare per l'inclusione dei dispositivi nella selezione.
4. 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.

Rete

Nella sezione **Rete** è possibile specificare i criteri che verranno utilizzati per includere i dispositivi nella selezione in base ai dati della rete:

- **Nome o indirizzo IP dispositivo**
- Dominio Windows

  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. Consente di visualizzare 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.

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.

- Il tag 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.

- Il tag 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.

Attività di rete

Nella sezione **Attività di rete** è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base alle relative attività della rete:

- Il dispositivo è un 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.

Applicazione

Nella sezione **Applicazione** 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 di amministrazione.

  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.

- 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 Kaspersky Security Center 14

  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.

Sistema operativo

Nella sezione **Sistema operativo** è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base al tipo di sistema operativo.

- Versione del sistema operativo

  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.

- 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.

- 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.

- 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.

- ID 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.

Stato dispositivo

Nella sezione **Stato dispositivo** 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*.

- 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*.

- Stato dispositivo definito dall'applicazione

  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.

Componenti della protezione

Nella sezione **Componenti della protezione** 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.

- Ultima scansione

  Se questa opzione è abilitata, è possibile eseguire la ricerca dei dispositivi client in base all'ora dell'ultima scansione virus. Nei campi di immissione è possibile specificare il periodo di tempo entro il quale è stata eseguita l'ultima scansione virus.

  Per impostazione predefinita, questa opzione è disabilitata.

- Numero totale di minacce rilevate

  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.

Registro delle applicazioni

Nella sezione **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 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.

Registro hardware

Nella sezione **Registro hardware** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'hardware installato:

- 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 CPU (MHz)

  L'intervallo di frequenze di una CPU. I dispositivi con CPU corrispondenti all'intervallo di frequenze in questi campi (compresi) verranno inclusi nella selezione.

- Core CPU virtuali

  Intervallo del numero di core virtuali in una CPU. I dispositivi con CPU corrispondenti all'intervallo in questi campi (compresi) verranno inclusi nella selezione.

- Volume disco rigido (GB)

  Intervallo di valori per le dimensioni del disco rigido nel dispositivo. I dispositivi con dischi rigidi corrispondenti all'intervallo in questi campi di immissione (compresi) verranno inclusi nella selezione.

- Dimensione RAM (MB)

  Intervallo di valori per le dimensioni della RAM del dispositivo. I dispositivi con RAM corrispondenti all'intervallo in questi campi di immissione (compresi) verranno inclusi nella selezione.

Macchine virtuali

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:

  - **Non importante**.
  - **No**. Vengono trovati i dispositivi che non sono macchine virtuali.
  - **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:

  - **Non importante**.
  - **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).

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, 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'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.

Problemi che influiscono sullo stato nelle applicazioni gestite

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.

Descrizione stato del dispositivo

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.

Stati dei componenti nelle applicazioni gestite

Nella sezione **Stati 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 di 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 di protezione dei server di posta (*Nessun dato dal dispositivo*, *Arrestata*, *Avvio in corso*, *Sospesa*, *In esecuzione*, *Non riuscito*).

- Stato Sensore Endpoint

  Cercare i dispositivi in base allo stato del componente Sensore Endpoint (*Nessun dato dal dispositivo*, *Arrestata*, *Avvio in corso*, *Sospesa*, *In esecuzione*, *Non riuscito*).

Componenti dell'applicazione

Questa sezione contiene un elenco dei componenti delle applicazioni per cui sono installati plug-in di gestione corrispondenti in Administration Console.

Nella sezione **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: *Nessun dato dal dispositivo*, *Arrestato*, *Avvio in corso*, *Sospeso*, *In esecuzione*, *Malfunzionamento* o *Non installato*. 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:

  - *Avvio in corso* - Il componente è attualmente in fase di inizializzazione.
  - *In esecuzione* - Il componente è abilitato e correttamente in esecuzione.
  - *Sospeso* - Il componente è sospeso, ad esempio dopo che l'utente ha sospeso la protezione nell'applicazione gestita.
  - *Malfunzionamento* - Si è verificato un errore durante l'esecuzione del componente.
  - *Arrestato* - Il componente è disabilitato e al momento non è in esecuzione.
  - *Non installato* - L'utente non ha selezionato il componente per l'installazione durante la configurazione dell'installazione personalizzata dell'applicazione.

  A differenza degli altri stati, lo stato *Nessun dato dal dispositivo* 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.

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 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).
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	Monitoraggio e generazione 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.	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 Server sugli Administration Server secondari	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
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.	Monitoraggio dell'esecuzione delle 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	Visualizzazione delle informazioni sulle chiavi di licenza in uso

	Administration Server. L'elenco contiene dati dettagliati su ogni chiave di licenza, tra cui nome, tipo o data di scadenza.	
Creare e trovare un utente interno	È possibile creare un account per utilizzi successivi.	Selezione dell'account per l'avvio di Administration Server
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 degli account utente

Applicazioni che interagiscono con Kaspersky Security Center tramite OpenAPI

Alcune applicazioni interagiscono con Kaspersky Security Center 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 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 OpenAPI. Per scoprire se l'applicazione in uso funziona con OpenAPI, vedere la Guida di tale applicazione.

Integrazione tra Kaspersky Security Center Web Console e altre soluzioni Kaspersky

Questa sezione descrive come configurare l'accesso da Kaspersky Security Center Web Console a un'altra applicazione Kaspersky, ad esempio Kaspersky Endpoint Detection and Response e Kaspersky Managed Detection and Response.

Configurazione dell'accesso a KATA / KEDR Web Console

Kaspersky Anti Targeted Attack (KATA) e Kaspersky Endpoint Detection and Response (KEDR) sono due blocchi funzionali di Kaspersky Anti Targeted Attack Platform. È possibile gestire questi blocchi funzionali tramite la console Web per Kaspersky Anti Targeted Attack Platform (KATA / KEDR Web Console). Se si utilizzano sia Kaspersky Security Center 14 Web Console che KATA / KEDR Web Console, è possibile configurare l'accesso a KATA / KEDR Web Console direttamente dall'interfaccia di Kaspersky Security Center 14 Web Console.

Per configurare l'accesso a KATA / KEDR Web Console:

1. Nella finestra principale dell'applicazione fare clic su **Impostazioni della console** nella parte superiore dello schermo.
2. Nel menu a discesa selezionare **Integrazione**.

   Verrà aperta la finestra Impostazioni della console.
3. Nella scheda **Integrazione**, immettere l'URL di KATA/KEDR Web Console nel campo **URL di KATA/KEDR Web Console**.
4. Fare clic sul pulsante **Salva**.

L'elenco a discesa **Gestione avanzata** viene aggiunto alla finestra principale dell'applicazione. È possibile utilizzare questo menu per aprire KATA / KEDR Web Console. Facendo clic su **Sicurezza informatica avanzata**, nel browser viene aperta una nuova scheda con l'URL specificato.

Stabilire una connessione in background

Per configurare l'interazione tra Kaspersky Security Center e un'altra applicazione o soluzione Kaspersky, ad esempio Kaspersky Managed Detection and Response (denominato anche MDR), è necessario stabilire una connessione in background tra Kaspersky Security Center Web Console e Administration Server. È possibile stabilire questa connessione solo se il proprio account dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti dell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

> È possibile configurare l'interazione solo tra Kaspersky Managed Detection and Response e la versione basata su Windows di Kaspersky Security Center.

Per stabilire una connessione in background:

1. Nell'elenco a discesa **Impostazioni della console** selezionare **Integrazione**.

   Verrà aperta la finestra **Impostazioni della console**.
2. Selezionare la scheda **Integrazione**.
3. Nella scheda **Integrazione** selezionare la sezione **Integrazione**.

4. Spostare l'interruttore per stabilire una connessione in background sulla posizione: **Stabilisci una connessione in background per l'integrazione ABILITATO**.

5. Nella sezione **Il servizio che stabilisce una connessione in background verrà avviato nel server Kaspersky Security Center Web Console** visualizzata fare clic sul pulsante **OK**.

Viene stabilita la connessione in background tra Kaspersky Security Center Web Console e Administration Server. Administration Server crea un account per la connessione in background e questo account viene utilizzato come account di servizio per mantenere l'interazione tra Kaspersky Security Center e un'altra applicazione o soluzione Kaspersky. Il nome di questo account di servizio contiene il prefisso NWCSvcUser. Administration Server cambia automaticamente la password dell'account di servizio ogni 30 giorni, per motivi di sicurezza. Non è possibile eliminare l'account di servizio manualmente. Administration Server elimina automaticamente questo account quando si disabilita una connessione tra servizi. Administration Server crea un singolo account di servizio per ogni Kaspersky Security Center 14 Web Console e Administration Console e assegna tutti gli account di servizio al gruppo di protezione con il nome ServiceNwcGroup. Administration Server crea automaticamente questo gruppo di protezione durante il processo di installazione di Kaspersky Security Center. Non è possibile eliminare questo gruppo di protezione manualmente.

Contattare il Servizio di 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. 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 del prodotto). 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

Ottenere assistenza tecnica telefonica

È possibile contattare gli specialisti del Servizio di assistenza tecnica dalla maggior parte delle aree geografiche di tutto il mondo. Nel sito Web del Servizio di assistenza clienti di Kaspersky , è possibile trovare informazioni su come ottenere assistenza tecnica nella propria area geografica e le informazioni di contatto del Servizio di assistenza tecnica.

Prima di contattare il Servizio di assistenza tecnica, consultare le regole dell'assistenza .

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.

Fonti di informazioni sull'applicazione

Pagina di Kaspersky Security Center nel sito Web di Kaspersky

Nella pagina di Kaspersky Security Center nel sito Web di Kaspersky sono disponibili informazioni generali sull'applicazione e le relative funzionalità e caratteristiche.

Pagina di Kaspersky Security Center 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 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:

- 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 non richiede l'immissione delle credenziali.
- L'attività *Cambia Administration Server* non viene avviata automaticamente dopo aver impostato l'opzione **Immediatamente** nella pianificazione delle attività e salvato le modifiche.
- Se si specificano le impostazioni del server proxy nelle proprietà dell'Administration Server, quindi si abilita l'opzione **Non utilizzare il server proxy** nell'attività *Scarica aggiornamenti nell'archivio di Administration Server*, questa opzione viene ignorata e la connessione viene stabilita tramite il server proxy.
- Se si apre Kaspersky Security Center 14 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.
- Si verifica un errore quando si tenta di ripristinare un oggetto dall'archivio **BACKUP** (**OPERAZIONI** → **ARCHIVI** → **BACKUP**) o inviare l'oggetto a Kaspersky.
- Le impostazioni bloccate in un criterio principale di Kaspersky Endpoint Security for Linux vengono ereditate, ma non bloccate nei criteri secondari.
- Le informazioni hardware inviate da un dispositivo gestito all'Administration Server potrebbero non essere complete; alcuni elementi hardware potrebbero non essere specificati.
- È possibile eliminare una categoria di applicazioni aggiunta alla funzionalità Controllo applicazioni nel criterio di Kaspersky Endpoint Security for Linux.
- 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.
- Se si specificano account utente personalizzati nei parametri webConsoleAccount e managementServiceAccount in un file di risposta per l'installazione di Kaspersky Security Center 14 Web Console e questi account appartengono a gruppi di sicurezza diversi, Kaspersky Security Center 14 Web Console non funzionerà dopo l'installazione.

- 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 14 Web Console.

Administration Server

Un componente di Kaspersky Security Center 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 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.

Aggiornamento

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

La persona che gestisce le operazioni dell'applicazione tramite il sistema centralizzato di amministrazione remota Kaspersky Security Center.

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 14 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 abbonamento aggiuntiva

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.

Gravità 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.

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 applicazioni concesse in licenza

Gruppo di applicazioni creato in base ai criteri impostati dall'amministratore (ad esempio, per produttore), per cui vengono registrate statistiche sulle installazioni nei dispositivi client.

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 (KSN Privato)

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 dell'utente 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 System Health Validator (SHV)

Un componente Kaspersky Security Center utilizzato per la verifica della possibilità di utilizzare il sistema operativo in caso siano in esecuzione contemporaneamente Kaspersky Security Center e Microsoft NAP.

Negozio applicazioni

Componente di Kaspersky Security Center. 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 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.

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 computer 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.

Server Web di Kaspersky Security Center

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, profili MDM iOS e file da una cartella condivisa.

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 di protezione della rete

Stato di protezione corrente, che definisce la sicurezza dei dispositivi della rete aziendale. Lo stato di 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 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. Nessun dato relativo agli utenti interni viene trasferito al sistema operativo. Kaspersky Security Center esegue l'autenticazione degli utenti interni.

Workstation di amministrazione

Un dispositivo da cui si apre Kaspersky Security Center 14 Web Console. Questo componente fornisce un'interfaccia di gestione per Kaspersky Security Center.

La workstation di amministrazione viene utilizzata per configurare e gestire la parte server di Kaspersky Security Center. Utilizzando la workstation di amministrazione, l'amministratore crea e gestisce un sistema centralizzato di 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 negli Stati Uniti e/o in altri paesi.

Apache e il logo con la piuma di Apache sono marchi di Apache Software Foundation.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple, 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. registrati negli Stati Uniti e in altri paesi e aree geografiche.

La parola, il marchio e i logo Bluetooth sono di proprietà di Bluetooth SIG, Inc.

Ubuntu è un marchio registrato di Canonical Ltd.

Cisco, 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 e XenServer sono marchi di Citrix Systems, Inc. e/o una o più delle relative filiali e possono essere registrati presso lo United States Patent and Trademark Office e 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.

Dropbox è un marchio di Dropbox, Inc.

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, Hangouts e YouTube sono marchi di Google LLC.

FusionCompute, FusionSphere sono marchi di Huawei Technologies Co., Ltd registrati in Cina e in altri paesi.

Intel, Core, Xeon sono marchi di Intel Corporation negli Stati Uniti e / o in altri paesi.

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.

Micro Focus è un marchio o un marchio registrato di Micro Focus (IP) Limited o delle relative consociate nel Regno Unito, 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, 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.

Novell è un marchio registrato di Novell Enterprises Inc. negli Stati Uniti e in altri paesi.

Oracle, Java, JavaScript e TouchDown sono marchi registrati di Oracle e/o delle relative consociate.

Parallels e il logo Parallels sono marchi o marchi registrati di Parallels International GmbH in Canada, negli Stati Uniti e/o altrove.

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, Ansible, CentOS, 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.

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.

VMware, VMware vSphere, VMware Workstation sono marchi o marchi registrati di VMware, Inc. negli Stati Uniti e/o in altre giurisdizioni.

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.